Metropolia

TEKNIIKKA JA LIIKENNE

Tietotekniikka

Tietoliikennetekniikka

INSINÖÖRITYÖ

KÄYTTÄJÄN AUTENTIKOINTI YRITYKSEN TIETOVERKOSSA RADIUS-PALVELINTA KÄYTTÄEN

Työn tekijä: Henrik Frank
Työn valvoja: Marko Uusitalo
Työn ohjaaja: Mika Kähärä

Työ hyväksytty: 21.1.2010

Marko Uusitalo
lehtori

ALKULAUSE

Tämä insinöörityö tehtiin DataCenter Finland Oy:lle. Kyseisestä yrityksestä kiitän Markku Mikkolaa työn aiheesta sekä työn ohjaaja Mika Kähärää avustamisesta työn teknisissä kysymyksissä.

Kiitän lämpimästi Anu Haapalaista työn oikolukemisesta ja avustamisesta sen kieliasun kanssa.

Lisäksi erityisesti kiitän avopuolisoani Laura Sorria sekä vanhempiani tuesta ja kannustuksesta insinöörityön tekemisessä sekä koko opiskeluaikana.

Helsingissä 6.1.2010

Henrik Frank

Metropolia

TIIVISTELMÄ

Työn tekijä: Henrik Frank

Työn nimi: Käyttäjän autentikointi yrityksen tietoverkossa RADIUS-palvelinta käyttäen

Päivämäärä: 16.1.2010 **Sivumäärä:** 53

Koulutusohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoliikennetekniikka

Työn ohjaaja: Lehtori Marko Uusitalo

Työn ohjaaja: Tietoliikennekonsultti Mika Kähärä

Tässä insinöörityössä on selvitetty verkkodokumenttien sekä kirjallisuuden avulla käyttäjä-autentikoinnin toteutus yrityksen tietoverkossa käyttäen AAA-protokollaa sekä sen toteutuksessa RADIUS-palvelinta. Työssä tutkitaan teoriatasolla AAA-protokollan sisältö sekä RADIUS-palvelimen toiminta ja asennettiin RADIUS-palvelin sekä testattiin sen toiminta.

Työssä esitellään yleisellä tasolla yrityksen tietoverkon toteutusvaihtoehdot sekä huomioitavat tietoturvakysymykset. Lisäksi esitellään erilaiset mahdollisuudet käyttäjätunnistuksen toteuttamiselle. Lopuksi asennetaan RADIUS-palvelin ja tutkitaan sen soveltuvuutta yrityksen tietoverkon käyttäjä-autentikoinnin toteutukseen.

Työn lopputuloksena voidaan esittää ratkaisumalli yrityksen sisäisen tietoverkon käyttäjä-autentikoinnin toteutukselle noin 10 käyttäjän yritysverkkoon.

Avainsanat: Tietoturva, AAA, Autentikointi, RADIUS

Metropolia

ABSTRACT

Name: Henrik Frank

Title: User authentication at Company Network using RADIUS-server

Date: 16.10.2010 **Number of pages:** 53

Department: Information Technology **Study Programme:** Telecommunications

Instructor: Senior Lecturer Marko Uusitalo

Supervisor: Telecommunications consult Mika Kähärä

The purpose of the thesis was to study user authentication methods in a corporate network using the AAA-protocol and implementing them on the RADIUS-server.

The first theoretical chapters introduce generally different network technologies and the methods how company networks are usually created in addition the information security issues and different connection and authentication protocols. The content of the AAA-protocol and the functions of the RADIUS-server are described introduced more specifically. The theoretical knowledge was based on literature and Internet documents regarding the topic.

The final chapters of this study describe the installation and testing of the RADIUS-server in a virtual network environment. The suitability of the RADIUS-server and its function alternatives for the initial purpose, user authentication methods in a corporate network, are also evaluated.

The final result of the thesis is to present a design for a company network in which user authentication is implemented with the RADIUS-server.

Keywords: Information Security, AAA, Authentication, RADIUS

SISÄLLYS

LYHENTEET

802.1Q	IEEE VLAN-Standardi.
802.1p	IEEE VLAN-priorisointistandardi.
AAA	Authentication, Authorization, Accounting. Todennus, valtuutus ja tilastointi.
ADSL	Asymmetric Digital Subscriber Line. Asymmetrinen digitaalinen tilaajalinja.
CFI	Canonical Format Identifier. TCI-kentän Ethernet-yhteensopivuuden määrittävä kenttä.
CHAP	Challenge/Handshake Authentication Protocol. Haaste-vaste autentikointiprotokolla.
DHCP	Dynamic Host Configuration Protocol. Protokolla IP-osoitteiden jakamiselle.
EAP	Extensible Authentication Protocol. Todennusprotokollan runko
EAPOL	EAP over LAN. Lähiverkoissa käytettävä EAP-ratkaisu.
EAPOW	EAP over WLAN. Langattomissa lähiverkoissa käytettävä EAP ratkaisu.
IEEE	Institute of Eletcrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö.
IP	Internet Protocol. Internet-protokolla.
ISDN	Integrated Services Digital Network. Piirikytentäinen puhelinverkkojärjestelmä.
LAN	Local Area Network. Lähiverkko.
LCP	Link Control Protocol. PPP-protokollan osa.
LEAP	Lightweight Extensible Authentication Protocol. Autentikointiprotokolla langattomaan toteutukseen.
NAS	Network Access Server. Verkkoon liityntäpiste RADIUS-protokollassa.
NCP	Network Control Protocol. Verkkoprotokollien konfigurointiprotokolla.

OTP	One Time Password. Yhden kirjautumisen mahdollistava salasana.
OSI	Open Systems Interconnection Reference Model. Tiedonsiirtoprotokollien yhdistelmä.
PAM	Pluggable Authentication Model
PAP	Password Authentication Protoco. Salasana-autentikoinnin protokolla.
PPP	Point-to-Point Protocol. Protokolla suoran yhteyden muodostamiseen verkkolaitteiden välillä.
PPPoE	Point-to-Point Protocol over Ethernet. Laajakaistaverkoissa käytettävä PPP-protokolla.
QoS	Quality of Service. Tietoliikenteen luokittelu ja priorisointi.
RADIUS	Remota Authentication Dial In User Service. Autentikoinnin suorittava palvelin.
SLIP	Serial Line Internet Protocol. Sarjaportteja sekä modeemiyhteyksille luotu internet-protokolla.
TACACS	Terminal Access Controller Access-Control System. Cisco Systemsin kehittämä autentikointiprotokolla.
TCI	Tag Control Information. Ohjaustietokenttä.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla.
TPID	Tag Protocol ID. Protokollatunnistekenttä.
UDP	User Datagram Protocol. Yhteyskäytäntö viestien välitykseen.
VID	VLAN identifier. TCI-kentän VLAN kehyksen määrittävä kenttä.
VLAN	Virtual Area Network. Virtuaalinen lähiverkko.
VPN	Virtual Private Network, Virtuaalinen yksityisverkko.
WAN	Wide Area Network. Alueverkko.
WWW	World Wide Web. Internetin palvelumuoto.

1 JOHDANTO

Nykyisessä yhteiskunnassa, jossa kaikki tiedonsiirto perustuu lähestulkoon kokonaan erilaisissa verkoissa tapahtuvaan liikenteeseen, on hyvin tärkeää pystyä kontrolloimaan eri käyttäjien suorittamia toimenpiteitä verkossa, jotta tiedonsiirron sekä verkossa tapahtuvan kanssakäymisen turvallisuus ja luotettavuus voidaan saattaa mahdollisimman pitkälle. Tällöin on tärkeää, että kyetään antamaan eri käyttäjille heidän tarvitsemat oikeudet eri verkon osille sekä myös valvomaan eri käyttäjien tekemisiä.

Haastavaksi verkkoliikenteen seuraaminen muodostuu, jos kyseessä on osittain julkinen verkko, kuten monissa yrityksissä nykyään on. Tällöin käytännössä kuka tahansa pääsee kytkeytymään yrityksen verkkoon ja sitä kautta mahdollisesti aiheuttamaan riskin tietoturvallisuuteen. Kuitenkaan tätä ulkopuolista liikennettä ei voida kokonaan estää, koska monesti yrityksissä vierailevien henkilöiden tulee päästä liittymään verkkoon väliaikaisesti. Tällaisissa tapauksissa, kuten myös verkon jatkuvien käyttäjien käytön kontrolloimisessa, voidaan tukeutua käyttämään ns. AAA-standardia, eli käyttäjän todennusta, valtuutusta sekä tilastointia.

Nykyisistä verkkosovelluksista erittäin yleinen tunnistusta ja valtuutusta vaativia www-palveluja ovat erilaiset verkkokaupat, joissa maksu voidaan suorittaa käyttämällä esim. luottokorttia. Tällöin myös tiedon oikeellisuus ja eheys pitää todentaa, jolloin todentamiseen tulee yksi elementti lisää.

Työn lähtökohtaisena tarkoituksena on tutkia yrityksen tietoverkkoon suunnattuja käyttäjän autentikointijärjestelmiä, joilla pystytään seuraamaan verkon liikennettä, jakamaan oikeuksia päästä eri verkkolaitteille sekä säilömään tiedot verkkoliikenteestä sekä tehdyistä muutoksista. Jotta verkon liikennettä sekä eri laitteelle tehtyjä muutoksia voidaan seurata ja kontrolloida, on tärkeää saada myös tallennettua verkon käyttäjäliikenteestä kertyvä data. Lisäksi pitää pystyä todentamaan tiedon eheys ja luotettavuus.

Insinöörityössä käydään läpi verkkoteknologiat, lähiverkkojen ja virtuaalisten lähiverkkojen toiminta, eri yhteysprotokollat, autentikointiprotokollat sekä niiden toimintaperiaate ja tarkoitus. Lisäksi esitellään RADIUS-palvelin yleisesti sekä käytännössä asennetaan ja testataan autentikoinnissa käytettävä RADIUS-palvelin.

Työn lopputuloksena on saada luotua toimiva autentikointjärjestelmä noin 10 käyttäjän yrityksen tietoverkkoon. Järjestelmä luodaan aluksi testiympäristössä ja lopullinen käyttöönotto yrityksessä tapahtuu myöhemmin. Työn pohjalta on tarkoitus kyetä tarjoamaan yritykselle luotettava tietoturvaratkaisu perustuen käyttäjän tunnistamiseen ja valtuuttamiseen.

2 YHTEYSTEKNOLOGIAT

Tässä luvussa esitellään lyhyesti käytössä olevia yhteysteknologiota ja niiden erilaisia siirto-ominaisuuksia. Aluksi käsitellään lyhyesti käytössä melko harvinaiset modeemi- ja ISDN-tekniikat sekä nykyään yksityis- ja yrityskäytössä hallitseva ADSL-tekniikka. Lisäksi luodaan katsaus mobiileihin yhteystekniikkaratkaisuihin, jotka muodostavat nykyään erittäin merkittävän datan siirtoratkaisun.

2.1 Modeemi ja ISDN

Modeemin käyttö mahdollistaa tietoliikenneyhteyden tietokoneiden välillä käyttämällä puhelinverkkoa. Modeemin toiminta perustuu datan muuttamiseen ääneksi, jolloin se voidaan siirtää puhelinverkossa toiseen tietokoneeseen. Nykyisillä standardeilla mitattuna modeemilla muodostettu yhteys on kuitenkin niin rajoittunut ja hidas, että se ei sovellu muuhun kuin korkeintaan sähköpostien lukemiseen tai muihin erittäin kevyisiin verkkosovelluksiin.

Myös ISDN-palveluverkko on nykyään jo lähestulkoon kokonaan käytöstä poistunut teknologia. ISDN-tekniikan valttina modeemiin verrattuna on puolta suurempi tiedonsiirtonopeus, mutta nykystandardeilla mitattuna myös ISDN on melko hidas, eikä näin ollen mahdollista raskasta verkkoliikennettä. ISDN-tekniikka perustuu myös puhelinverkon käyttöön tiedonsiirrossa, mutta poiketen modeemiyhteydestä, ISDN-yhteys on puhtaasti digitaalinen.

ISDN-yhteys on mahdollista toteuttaa käyttämällä kahta eri liittymätyyppiä: perusliittymää tai järjestelmäliittymää. Perusliittymä on tarkoitettu lähinnä kotitalouskäyttöön, kun taas järjestelmäliittymä yrityskäyttöön. Liittymien suurin ero on tiedonsiirtokapasiteetissä. [1. 68-70]

2.2 ADSL

Internetin käytön erittäin voimakas kasvu viimeisen kymmenen vuoden aikana on kasvattanut tarvetta entistä suorituskykyisempien tiedonsiirtotekniikoi-

den kehittämiselle. Erilaiset verkkosovellukset, multimedia sekä kasvaneet tiedostokoot ovat saaneet aikaan sen, että kuluttajat tarvitsevat suorituskykyistä tiedonsiirtoa mahdollisimman edullisesti. Koska edellä mainittujen teknologioiden toiminta perustui puhelinverkkoihin, ei niiden suorituskyvyn nostaminen onnistu tämän päivän vaatimusten tasolle, joten niiden paikan on jokapäiväisessä kuluttajakäytössä korvannut ADSL-liittymät. ADSL-tekniikka perustuu myös käytännössä puhelinverkon kuparikaapeleihin, mutta se tarjoaa huomattavasti paremman ja suorituskykyisemmän tiedonsiirtoratkaisun kuin edellä mainitut teknologiat. Koska ADSL-yhteys käyttää samaa liittymää kuin normaali puhelinyhteys, asettaa liittymä tiettyjä rajoituksia ADSL-yhteyden tiedonsiirrolle. Näitä ovat esimerkiksi tilaajakaapelin pituus sekä kunto. Tämä ongelma ilmenee eritoten taajamien ulkopuolella.

ADSL-yhteyden muodostamiseen tarvitaan kuparikaapelin molempiin päihin ADSL-modeemi. Jotta puhelinverkko jää siihen käyttöön, mihin se on alun perin suunniteltu, eli puhelinliikenteeseen, erotetaan taajuusaluuet ADSL-yhteydelle ja puhelinverkolle käyttämällä erotussuodinta.

Kuten ADSL-yhteyden nimestä käy ilmi, on yhteys epäsymmetrinen, eli sen siirtonopeus on käyttäjän suuntaan suurempi kuin käyttäjältä verkkoon päin. Tämän takia ADSL sopii erityisen hyvin esim. yksityiseen kotitalouskäyttöön. [1. 72-75]

2.3 Kaapelimodeemi

Kaapelimodeemi käyttää edellisistä tekniikoista poiketen siirtotienään kaapeli-TV-verkkoa. Käytännössä siis kaapelimodeemi liitetään kaapeli-TV-verkkoon, eikä puhelinverkkoon kuten aiemmat esitellyt tekniikat. Tämä mahdollistaa teoriassa huomattavasti nopeammat siirtoyhteydet, mutta käytännössä nopeudet ovat tällä hetkellä lähes verrattavissa ADSL-tekniikan tarjoamiin nopeuksiin. Teoriassa kaapeliverkon kautta voidaan saavuttaa 35 Mbps, mutta käytännössä nopeus jää olosuhteista riippuen n. 2-10 Mbps:iin.

Kaapelimodeemin suurin hyöty on nopeuden lisäksi se, että se jättää puhelinliittymän vapaaksi ainoastaan puhelinliikennettä varten. Lisäksi kaapelimodeemi ei häiritse normaalia television käyttöä.

Vaikka kaapelimodeemin toiminta muistuttaa perusperiaatteiltaan hyvin paljon analogisten modeemien toimintaa, pystyy se kuitenkin tarjoamaan huo-

mattavasti suuremmat siirtonopeudet. Käyttäjän suuntaan (downstream) dataa saadaan siirrettyä verkosta teoriassa jopa 400 Mbps:in nopeudella, kun taas käyttäjältä verkkoon (upstream) teoreettinen nopeus voi olla 108 Mbps:ssa. Todellisuudessa se asettuu välille 320 kbps - 10 Mbps. Nämä nopeudet ovat huomattavasti analogisen verkon tarjoamia mahdollisuuksia suuremmat.

Kaapeliverkkoon perustuva tietoliikennetekniikka on nykyään hyvin suosittua kaupunki- ja taajama-alueilla, joissa kaapeli-TV-yhtiöt tarjoavat Internet-palveluita puhelinyhtiöiden rinnalla. [1. 72-75]

2.4 Mobiililaajakaista

Tämän hetken ehkä eniten kasvava tietoliikennetekniikka on matkapuhelinverkon kolmatta sukupolvea (3G) hyödyntävä teknologia. Mobiililaajakaista perustuu kolmannen sukupolven matkapuhelinverkon mahdollistavaan laajakaistatasoiseen tiedonsiirtoon. Mobiililaajakaista mahdollistaa Internetin ja muiden verkkosovellusten käytön kaikkialla matkapuhelinverkon peittoalueella. Periaatteessa 3G-verkkoyhteyden pitäisi mahdollistaa raskaampienkin verkkosovellusten käyttämisen, mutta todellisuudessa vielä verkon laajuus ei mahdollista raskaiden verkkosovellusten käyttämisen.

3 LÄHIVERKKO JA VIRTUAALINEN LÄHIVERKKO

Tässä kappaleessa käsitellään lähiverkkoa (LAN), sen rakennetta sekä sen eri variaatioita. Lähiverkko itsessään on pienelle maantieteelliselle alueelle rajattu tietoliikenneverkko, johon voidaan kytkeä vaihteleva tarpeellinen määrä käyttäjiä. Lähiverkko voi olla yksinkertaisuudessaan yhden talouden koneiden muodostama verkko tai pienen toimiston sisäinen tietoverkko. Lähiverkot yhdistetään toisiinsa alueverkoilla (WAN). [2. 3-4]

Myös tämän työn tiimoilta tutkittava yrityksen tietoverkko perustuu hyvin pitkälti lähiverkkojen toimintaan, ja tämän myötä tässä kappaleessa esitellään lähiverkkoa ja sen eri sovelluksia ja toimintaperiaatetta. Lähiverkko voi olla myös langaton sovellus, jolloin mukaan astuu eri langattoman lähiverkon verkkostandardit.

3.1 Lähiverkko

Lähiverkko (LAN) tarkoittaa tietoliikenteessä verkkoa, joka on maantieteellisesti rajattu pienehkön alueen sisäpuolelle. Yleisesti lähiverkko on yhden organisaation hallinnassa, eli esimerkiksi yhden yrityksen tai yrityksen osan. Yksinkertaisesti sanottuna lähiverkko koostuu seuraavista komponenteista: kaapeleista, verkkolaitteista, työasemista sekä palvelimista.

Lähiverkon lähtökohtainen tarkoitus on saattaa tiedostojen siirto sekä eri laitteiden toiminta samaan verkkoon mahdollisimman tehokkaasti. Yksinkertaistetusti voi todeta, että lähiverkon tehtävänä on tarjota käyttäjilleen keskitetysti tiedostojen siirto- ja jakopalvelut, laiteresurssien jako, sanomanvälityspalvelut sekä muita yhteyspalveluita.

Lähiverkon kaksi tärkeintä laitetyyppiä ovat työasemat ja palvelimet. Työasemilla käytetään verkossa jaettavia tiedostoja ja laiteresursseja, joita palvelimet jakavat verkon käyttäjille. Yleisesti yritysten sisäisissä lähiverkoissa suosituin toimintamalli on se, että työasemissa on oma paikallinen käyttöjärjestelmänsä ja palvelimissa omansa, mutta niin, että nämä kykenevät toimimaan yhdessä tehokkaasti. Tiedostoja ja hakemistoja jakavat palvelimet (fileserver) ovat erikoistuneet tiedostojen sekä yhteisten sovellusten jakamiseen ja varastoimiseen. Oheislaitteita, kuten tulostimia ja skannereita jakavat palvelimet (esim. print server) jakavat laitteita verkon käyttäjien kesken niin, että palvelut voidaan keskittää esim. yhdelle koneelle koko toimiston sisällä.

Tyypillisiä lähiverkkojen toteutuksessa käytettyjä palvelintuotteita ovat mm. Microsoftin SQL Server, Oracle sekä erilaiset Linux-toteutukset. Yrityskäyttöön on tarjolla varta vasten suunniteltuja työryhmäratkaisuita, kuten esimerkiksi Microsoft Exchange, jolla saadaan keskitettyä yrityksen sähköposti ym. palvelut helposti hallittavaksi kokonaisuudeksi. [3. 4-21]

Teknisesti lähiverkko toteutetaan usein normaalilla parikaapelilla, joskin nykyään toteutukselle on olemassa muitakin vaihtoehtoja, kuten valokuitu-, radioaalto- ja infrapunasädeverkko. Tosin jälkimmäinen on hyvin harvinainen eikä yleisesti käytetty vaihtoehto.

Lähiverkko rakentuu kaapeloinnista eli topologiasta. Yleisimpinä toteutusvaihtoehtoina on kolme erilaista topologiaa: väylä, rengas tai tähti. Näitä to-

pologioita voidaan myös yhdistellä, jonka seurauksena saadaan aikaiseksi hybridiratkaisuita.

Verkkotopologioista puhuttaessa on huomioitava, että käytössä on kaksi topologiamallia: fyysinen topologia ja looginen topologia. Fyysinen topologia kuvaa verkon fyysistä rakennetta, eli miten verkko on kaapeleiden yms. laitteiden sijoittelulla rakennettu. Looginen topologia puolestaan kuvaa verkon toimivuutta ja sitä, kuinka tieto kulkee laitteiden välillä käyttäjältä toiselle, ilman, että fyysinen laitesijoittelu tai kaapelointi on tarkemmin kuvattuna. Seuraavissa kappaleissa esitellään yksityiskohtaisemmin eri lähiverkkotopologiat. [3. 4-21]

3.1.1 Väylätopologia

Väylätopologia on looginen topologia, joka perustuu rakenteeseen, jossa samaa siirtokanavaa käytetään kaikkien verkossa olevien laitteiden kesken. Tällöin tieto siirtyy kaikkien verkkolaitteiden välillä samaa kanavaa pitkin samanaikaisesti. Verkossa ei ole erikseen määrättyä kulkusuuntaa siirrettävälle tiedolle, vaan se kulkee kaikkiin suuntiin. Haaroittamattomassa väylässä tieto eli kehys siirtyy kahteen suuntaan, kun taas haaroitetussa verkossa tieto kulkee kaksisuuntaisesti jokaiseen haaraan. Yksinkertaisesti ajateltuna väylätopologiaa voidaan pitää äärettömän pitkänä kaapelina, joka yhdistää eri laitteet toisiinsa. [3. 66-98]

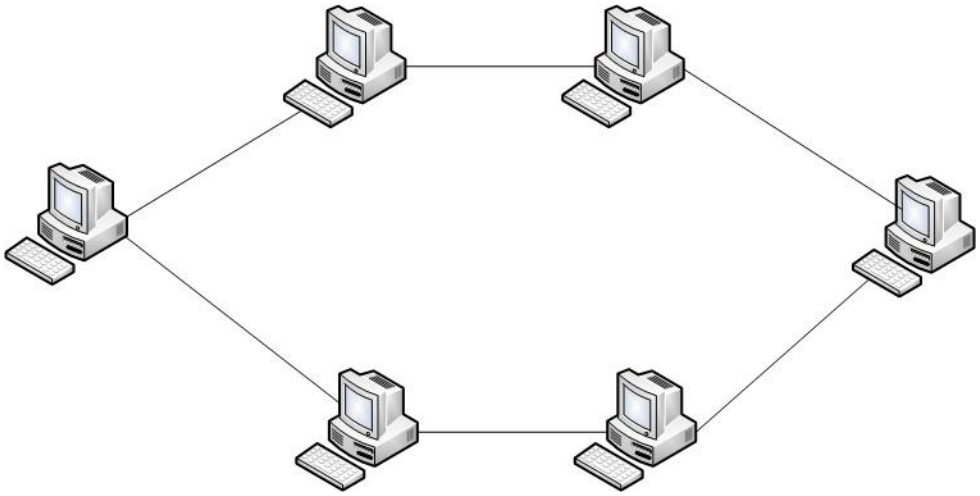
Kuva 1. Väylätopologia

3.1.2 Rengastopologia

Rengastopologiassa laitteet kytketään renkaan muotoiseen verkkoon. Kyseessä on looginen topologia. Tällöin tieto kulkee vuorottain jokaisen laitteen läpi käyttäen samaa kiertosuuntaa verkon sisällä. Verkon kiertosuunnaksi on yleisesti määritelty käytettäväksi myötäpäiväistä dataliikennettä. Rengasverkon etuna on se, että tiedon saapuminen eri laitteille sekä sen liikkuminen pystytään määrittelemään tarkasti verrattuna väylätopologian liikenteeseen. Toisin kuin väylätopologiassa, jossa verkko on periaatteessa äärettömän pitkä kaapeli, rengas on äärellinen, jolloin kehyksen (tiedon) saapumishetki kullekin koneelle voidaan laskea tarkasti. Renkaan äärellisyydestä johtuen siir-

rettävä kehys tulee poistaa renkaasta, jottei se jää kiertämään verkkoa loputtomasti estäen verkon käyttöä. Käytännössä tämä toteutetaan niin, että kehyksen lähettänyt kone poistaa sen verkosta sen palatessa lähettäjälle.

Rengastopologiaa käyttävä verkko on melko haavoittuvainen erilaisille laitehäiriöille, koska yhden laitteen toimimattomuus aiheuttaa koko verkon toiminnan katkeamisen. Lisäksi laitteiden lisääminen verkkoon on työläämpää kuin esimerkiksi seuraavaksi esiteltävässä tähtitopologiaa soveltavassa verkkoratkaisussa. [3. 66-98]

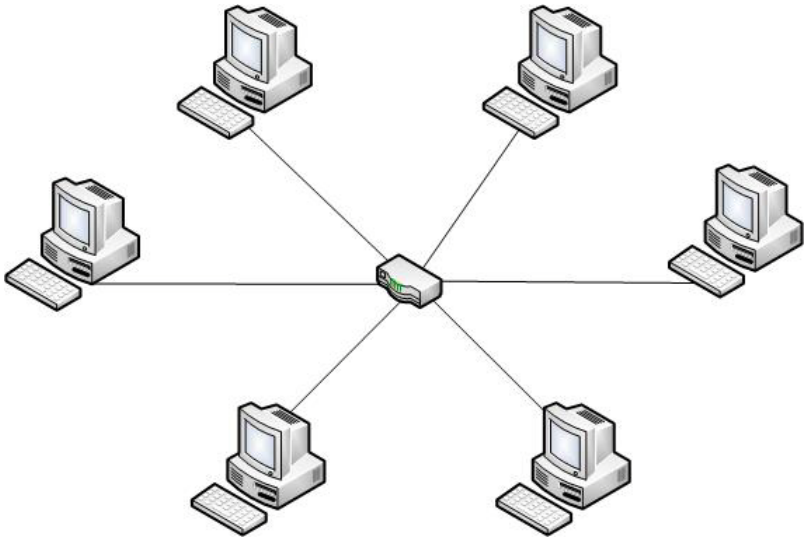


Kuva 2. Rengastopologia

3.1.3 Tähtitopologia

Fyysinen tähtitopologia perustuu yhteen keskuslaitteeseen, joka jakaa yhteydet muiden verkossa olevien laitteiden kesken. Tämä koko verkon käyttäjiä yhdistävä ”keskipiste” on verkon aktiivilaite eli keskitin, kytkin tai reititin. Kyseinen verkkomalli on nykyään ylivoimaisesti suosituin fyysinen verkkotopologia lähiverkon toteutuksessa.

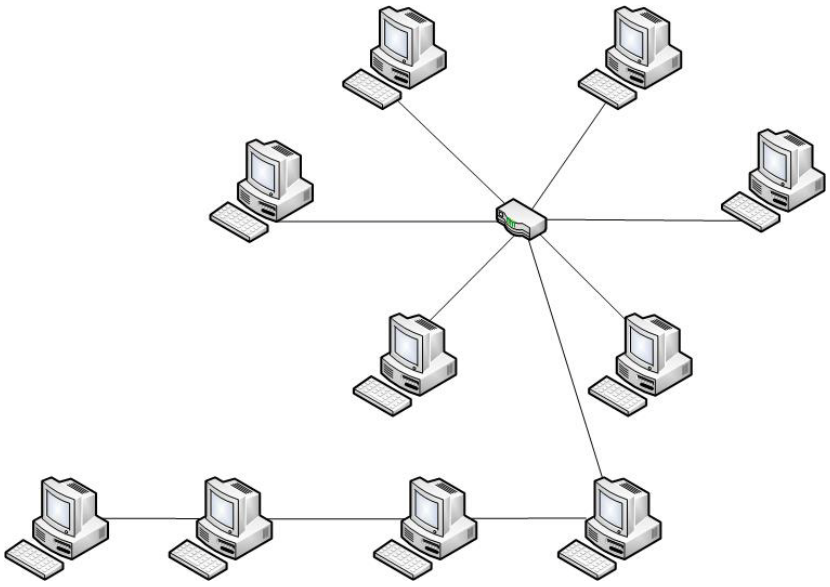
Käytännössä verkko toimii niin, että jokainen verkossa oleva työasema kommunikoi ja siirtää tietoa verkon sisällä tämän keskuslaitteen kautta. Tällöin esimerkiksi yhden laitteen ongelmatilanne tai laitteen lisääminen tai poistaminen ei haittaa muun verkon toimintaa. Tähtiverkon toiminnan voi katkaista ainoastaan keskuslaitteen toimimattomuus. Tämän takia kyseinen malli on esitellyistä vaihtoehdoista kaikkein toimintavarmin sekä helpoin ylläpitää. [3. 66-98]



Kuva 3. Tähtitopologia

3.1.4 Hybridi

Hybridiverkko on nimensä mukaisesti edellä mainittujen ratkaisuiden yhdistelmä. Tällaiseen ratkaisuun päädytään yleisesti esimerkiksi yrityksen sisällä tapahtuvien muutostöiden yms. seurauksena. Hybridiverkko ei ole yleisesti mikään pysyvä verkkoratkaisu, koska sen rakenteesta johtuva ylläpidon hankaluus vähentävät sen toiminnallisuutta ja tehokkuutta. [1. 32]



Kuva 4. Tähti- ja väylätopologian yhdistelmä

3.2 Virtuaalinen lähiverkko

Yleisin yritysmaailmassa käytettävä lähiverkkojen tekniikka on virtuaalinen lähiverkko VLAN. Virtuaalisessa lähiverkossa tietoliikenneverkko voidaan ja-

kaa pienempiin loogisiin osiin laitteiden fyysisestä sijainnista riippumatta, kunhan vain laitteet ovat ylipäänsä samassa verkossa. Verkko jaetaan laitteiden kesken ns. loogisiin osiin esimerkiksi yrityksen eri osastojen kesken. Virtuaalinen lähiverkko ratkaisuna helpottaa esimerkiksi tapauksessa, jossa yrityksen saman osaston työntekijöiden työpisteet sijaitsevat rakennuksessa fyysisesti eri paikoissa tai jopa täysin toisella puolella kaupunkia, mutta kuitenkin samassa lähiverkossa. [2. 155]

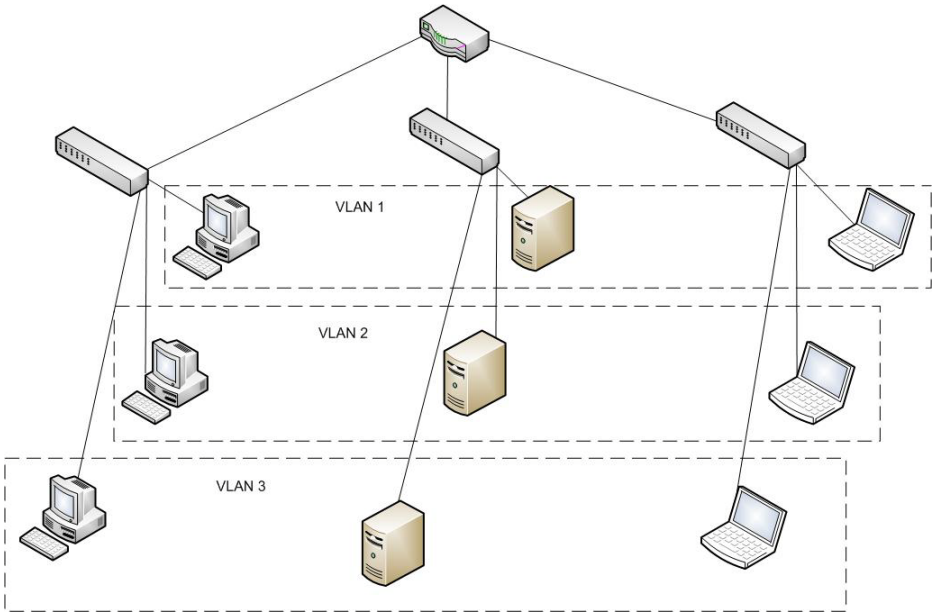
Kun kaksi tai useampia yrityksen verkkoja halutaan yhdistää, käytetään VPN-ratkaisua, jolloin kyseiset verkot muodostava näennäisesti yhteisen verkon.

Virtuaalisen lähiverkon rakentaminen voidaan karkeasti perustella seuraavilla asioilla:

- Lähiverkon tietoturva ei ole riittävä.
- Lähiverkon tiedonsiirtokapasiteetti ei ole riittävä.
- Halutaan rajoittaa lähiverkkoliikennettä.
- Halutaan keskittää tietyt verkkopalvelut vain tietyille käyttäjille.
- Halutaan helpottaa lähiverkon levitysviestien (broadcast) hallintaa.
- Halutaan helpottaa ylläpitoa.

Virtuaalinen lähiverkko toteutetaan käytännössä käyttämällä kytkimiä ja reitittimiä. Näillä määritellään lähiverkkoon toisistaan riippumattomia ryhmiä, joiden liikenne tapahtuu samassa fyysisessä verkossa, mutta niin, että tieto on käytettävissä vain samassa virtuaaliverkossa olevilla käyttäjillä. Näin pystytään siis esimerkiksi hallinnoimaan eri käyttäjien oikeuksia eri tietoihin yrityksen sisällä.

Virtuaalisessa lähiverkossa kaikki pakettipohjainen liikenne tapahtuu samassa aliverkossa sekä broadcast-alueessa olevien laitteiden välillä. Jos liikenne halutaan laajentaa kyseisen lähiverkon ulkopuolelle, tulee reititys suorittaa uudestaan lähiverkkojen välillä, koska jokainen virtuaalinen lähiverkko on oma looginen verkkonsa.



Kuva 5. Virtuaalisen lähiverkon rakenne

Virtuaalinen lähiverkko voidaan toteuttaa teknisesti ainakin neljällä eri tavalla. Tavallisesti VLAN:in määrittelyperusteet ovat seuraavat:

1. MAC-osoite
2. kytkimen portti
3. verkko-osoite
4. tietollikenneprotokolla.

MAC-osoitteeseen perustuva VLAN

MAC-osoitteeseen perustuvassa virtuaalisessa lähiverkossa määritellään MAC-osoitteet, eli laitteet, jotka kuuluvat samaan VLAN:iin ja näistä muodostetaan oma alueensa, jonka sisällä dataa siirretään. Tässä määrittelyssä samat laitteet voivat kuulua useaan virtuaalisen lähiverkkoon samaan aikaan. Ongelmana tämän tyyppisessä ratkaisussa on kuitenkin verkon hallittavuus, koska jokaiselle laitteelle tulee määritellä erikseen se, mihin VLAN:iin se kuuluu. [3. 93-99]

Kytkimen porttimäärityksiin perustuva VLAN

Kytkimen porttimäärityksiin perustuvassa virtuaalisessa lähiverkossa määritellään kukin kytkimen portti kuulumaan tiettyyn VLAN:iin. Tässä menetel-

mässä kukin työ-asema voi kuulua vain yhteen VLAN:iin, mutta toisaalta koska itse laitteen MAC-osoitetta ei huomioida, voidaan mikä tahansa laite liittää verkkoon ilman uudelleenmäärityksiä. Tämä helpottaa käyttäjää, jolla on käytössä useampi eri tietokone joita verkkoon tulee vaihtelevasti liittää. Toisaalta kyseisessä ratkaisussa tietoturva ja verkon seuranta on hankalampaa toteuttaa. Toteutus tässä määritelmässä on sinänsä hyvin helppoa, koska erikseen ei tarvitse määrittää jokaisen laitteen MAC-osoitetta. [3. 93-99]

Verkko-osoitteeseen perustuva VLAN

Verkko-osoitteeseen perustuva virtuaalisen lähiverkon määrittelyperuste on se, että samat IP-aliverkot sekä verkko-osoitteet ovat samassa VLAN:issa. Tämä tarkoittaa käytännössä sitä, että verkossa kukin protokolla muodostaa oman virtuaalisen lähiverkon. Hallittavuudeltaan kyseinen määritys on kuitenkin kohtalaisen helppo, koska kytkimet pystyvät suoriutumaan itse uudelleenmäärityksen verkon sisällä mahdollisten laitesiirtojen yhteydessä. Kyseinen malli ei ole enää nykyään kovinkaan yleisesti käytössä. [3. 93-99]

Tietoliikenneprotokollaan perustuva VLAN

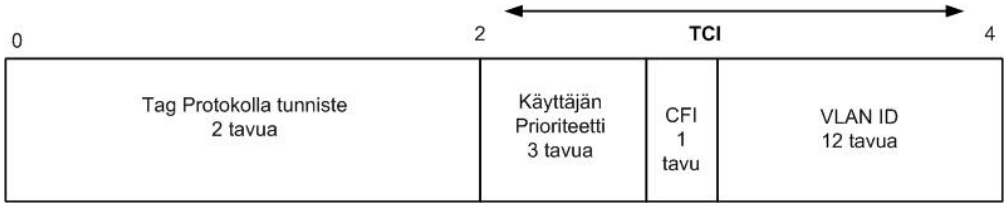
Tämä ns. Policy-perusteinen virtuaalisen lähiverkon toteutusmalli perustuu käyttäjien ryhmittelyyn eri perusteilla. Näitä perusteita voivat olla esimerkiksi verkko-osoite, käytettävän protokollan tyyppi tai muita protokollan sisältämiä tietoja. Ongelmana tässä määritelmässä on se, että tällöin VLAN:t saattavat olla käyttäjämäärältään hyvin epätasapainoisia, koska eniten käytetty protokolla muodostaa suoraan oman virtuaalisen lähiverkkonsa. Kuten edeltävä VLAN malli, tämäkään ei ole yleisesti enää juurikaan käytössä. [3. 93-99]

3.3 VLAN-standardit

Virtuaalisen lähiverkon toteutus nojaa yleisesti kahteen IEEE:n määrittämään standardiin, jotka ovat IEEE 802.1Q sekä IEEE 802.1p. Kyseiset standardit mahdollistavat lähiverkossa porttikohtaisen liikenteen seuraamisen ja autentikoinnin. Kyseiset standardit soveltuvat erityisesti käytettäväksi virtuaalisissa lähiverkkoratkaisuissa, mutta myös muissa mahdollisissa verkkoratkaisuissa. Tässä kappaleessa esitellään tarkemmin nuo edellä mainitut standardit.

3.3.1 IEEE 802.1Q

IEEE 802.1Q-standardi määrittelee kytkimen toiminnallisen arkkitehtuurin sekä Ethernet-kehysrakenteen, jota useimmat nykyiset 100 Mbps- ja 1Gbps-kytkimet tukevat. Kyseisessä standardissa Ethernet-kehykseen lisättiin mahdollisuus virtuaaliverkkoihin. Standardissa VLAN-kehyksen muodostaa kaksi 2 tavun kokoista lisäkenttää, jotka ovat TAG-protokollatunniste (TPID) sekä TAG-ohjaustiedosto (TCI).



Kuva 6. VLAN-kehyksen rakenne

Nämä lisäkentät yhdessä muodostavat virtuaalisen lähiverkon kehyksen, joka sisältää tyyppiarvon Ethernetille, joka puolestaan tunnistaa kehyksen 802.1Q-kehykseksi.

Kuten edellä todettiin, on TAG-protokollatunnisteen koko 2 tavua, joka sisältää myös niin sanotun Ethernet-tyyppiarvon (Ethertype), jonka arvona on heksaluku 0x8100.

TCI-ohjaustiedosto jakautuu kolmeen kolmeen eri osaan, jotka ovat IEEE 802.1p-standardin mukainen kolmen bitin prioriteettikenttä, yhden bitin kokoinen CFI-kenttä sekä yhden bitin kokoinen varsinainen VLAN ID (VID).

CFI-kentän tarkoituksena on yhdistää Ethernet- ja Token Ring-verkkoja samaan virtuaalisen lähiverkkoon. Ethernet-verkoissa tuon kentän arvon tulee olla aina nolla. Jos kehyksen arvo on yksi, kyseistä kehystä ei lähetetä eteenpäin.

VID-kenttä on 12 bitin mittainen numerotunniste, joka yksilöi aina kunkin virtuaalisen lähiverkon. Jos VID:n arvo on nolla, kyseinen kehys ei kuulu mihinkään virtuaaliseen lähiverkkoon. [4.]

3.3.2 IEEE 802.1p

Edellisessä kappaleessa jo viitattiin IEEE 802.1p-standardiin, jonka pääasiallisena tehtävänä on priorisoida liikennettä virtuaalisessa lähiverkossa. Ku-

ten edellisessä kappaleessa todettiin, on 802.1p 3 bitin mittainen, ja se toimii OSI-mallin toisen kerroksen MAC-alikerroksella. Kyseinen standardi tukee QoS-palvelua, joka luokittelee ja priorisoi verkkoliikennettä. QoS priorisoi liikennettä sen laadun ja verkon kantokyvyn mukaan, eli se osaa pudottaa pois esim. verkkoa hidastavat tekijät. Pelkästään 802.1p kentän käyttö ei kuitenkaan yksinään riitä liikenteen priorisointiin, vaan se toteutuu yhteydessä QoS-palvelun kanssa. Liikennettä voidaan luokitella myös sovellusten ja laitteiden perusteella.

802.1p-standardi muodostuu kolmen bitin kentästä, joiden perusteella liikenne voidaan jakaa priorisoinnin mukaan kahdeksaan eri tasoon. Kentät numeroidaan välillä 0-7, joista 7 taso on kaikkein suurin prioriteetti. Kenttä no. 7 verkon kannalta kriittisimmille toiminnoille sekä ylläpidolle. Yleisesti paras käytössä oleva kenttä on 6, kun taas vähiten merkitsevä kenttä 0. Tämä on niin sanottu ”Best effort” –arvo. [4.]

3.4 VLAN-tietoturvaratkaisut

Peruste virtuaalisen lähiverkon luomiselle on yleensä palveluiden keskittäminen sekä niiden hallinnoimisen helpottaminen. Toisena erittäin tärkeänä päämääränä ja saavutettuna etuna virtuaalisen lähiverkon toteutuksessa on tietoturvan lisääminen.

Koska virtuaalinen lähiverkko toteutetaan esimerkiksi tietyn yrityksen sisällä, kyetään sen käyttäjiä sekä käyttäjien verkkoliikennettä kontrolloimaan hyvin tarkasti. Tällöin muutokset sekä mahdolliset hyökkäykset kyetään tunnistamaan sekä ehkäisemään hyvin tehokkaasti. Verkkoon voidaan esimerkiksi toteuttaa halutunlainen autentikointijärjestelmä, jolla pystytään rajoittamaan käyttäjien pääsyä vain haluttuihin verkon osiin sekä estämään ulkopuolisten pääsy verkkoon. Autentikointijärjestelmän toteutukseen voidaan valita esimerkiksi RADIUS-autentikointijärjestelmä, joka esitellään tässä työssä tarkemmin myöhemmissä luvuissa. Vaikka VLAN:illa pyritään tehostamaan myös tietoturvallisuutta, ei se rakenteestaan huolimatta ole mitenkään täydellisen suojattu mahdollisilta tietoturvaongelmilta.

Virtuaalisissa lähiverkoissa verkon asetukset ja konfigurointi muodostavat erittäin tärkeän tekijän tietoturvan suhteen. Jos konfigurointi on tehty hyvin, virtuaalinen lähiverkko on tietoturvallinen, mutta jos asetukset on tehty huonosti, on verkko erittäin arka hyökkäyksille.

VLAN-hyökkäyksiä ovat esimerkiksi ns. VLAN-hyppely, jossa paketoidaan kaksi 802.1Q-kehystä yhteen, näin päästään käsiksi toiseen VLAN:iin. Tämä hyökkäys on mahdollista kuitenkin vain tiettyä topologiaa käyttävissä VLAN:eissa.

Toinen mahdollinen tapa hyökätä VLAN:iin on hyökkääjän toimesta tekeytyä joksikin verkon aktiivilaitteeksi, esim. kytkimeksi , tällöin keskustellaan VLAN-hallintaprotokollan kanssa ja tämän myötä päästään kiinni muihin verkon laitteisiin. [10.]

Tietoturvan kannalta kaikkein paras ratkaisu VLAN:in toteutukselle on MAC-osoitteisiin perustuva VLAN, mutta sen toteuttaminen on myös kaikkein monimutkaisin, koska tällöin esim. laitteiden lisääminen ja poistaminen on hyvin työlästä. Yksinkertaisin tapa ehkäistä riskejä on hoitaa virtuaalisen lähiverkon konfigurointi asianmukaisesti sekä välttää turhia palveluita, jotka mahdollistavat tietoturva-aukkojen kasvamisen VLAN:issa. [5.]

4 YHTEYSPROTOKOLLAT

Aiemmissa kappaleissa esitetyt verkkoteknologiat sekä rakenteet tarjoavat fyysisesti yhteyden käyttäjille sekä pääsyn internettiin. Näiden fyysisten rakenteiden lisäksi tarvitaan tiedonsiirtoon jokin yhteinen menetelmä, jolla tietoa siirretään. Tätä yhteistä menetelmää kutsutaan protokollaksi, joka määrittelee tavan, jolla pakettipohjaista tietoa siirretään verkossa. Käyttäjälle yhteysprotokolla on sinällään näkymätön, mutta niiden myötä kyetään määrittämään mm. yhteyden tietoturva sekä käyttäjien tunnistus.

Internetissä käytetään yleisesti verkkokerroksen protokollana TCP/IP-protokollaa, joka perustuu siihen, että dataa välitetään pakettimuodossa. Koska verkon tehtävänä on yksinkertaisesti vain välittää paketteja paikasta toiseen mahdollisimman tehokkaasti kiinnittämättä sen suuremmin huomiota niiden perillemenoon tai turvallisuuteen, ei TCP/IP-protokollaa voida pitää erityisen luetettavana tai tietoturvallisen yhteysprotokollana. Lisäksi TCP/IP-protokollaan ei ole sisällytetty mitään kuittausmekanismia, jolla liikennettä kyettäisiin seuraamaan. [1. 48-50]

TCP-protokolla toimii kerroksessa neljä ja IP-protokolla kerroksessa kolme, ja näiden päällä toimii eri sovelluksille sopivammat protokollat, joilla pysty-

pystytään tarjoamaan turvallinen käyttäjien autentikointi, valtutuutus sekä tilastointi.

Tässä kappaleessa esitellään PPP-protokollan toiminta sekä siihen liittyvät autentikointiprotokollat CHAP, EAP sekä PAP.

4.1 PPP-protokolla

Ensimmäinen puhelinverkossa tapahtuvaa tiedonsiirtoa varten luotu tiedonsiirtoprotokolla oli SLIP-protokolla, joka ei kuitenkaan toiminnaltaan ollut rajoitustensa vuoksi mitenkään kehuttava. SLIP-protokollan ensimmäinen heikko tekijä oli se, että se tuki vain ja ainoastaan TCP/IP-protokollaa, jolloin sen toiminta oli hyvin rajoitettua. Toisena heikkona tekijänä oli SLIP-protokollan rajoittuneisuus DHCP:n suhteen, eli se tuki ainoastaan järjestelmän kiinteää IP-osoitetta. Nykyisessä verkkomaailmassa tämä on erittäin kriittinen puute, koska IP-avaruus ei yksinkertaisesti riitä siihen, että kaikilla käyttäjillä olisi kiinteä IP-osoite. Lisäksi SLIP-protokollan heikkoutena oli erittäin hankala konfiguroitavuus. [6.]

Käytännön tasolla SLIP-protokolla ei ole millään muotoa ajankohtainen, mutta siihen kuitenkin perustuu nykyään käytössä oleva PPP-protokolla, jossa on otettu huomioon nykypäivän vaatimukset huomattavasti tehokkaammin. PPP-protokollan kehitys lähti liikkeelle SLIP-protokollan puutteellisuudesta. Käytännössä PPP korjaa kaikki SLIP-protokollan puutteet ja on näin ollen syrjäyttänyt sen täydellisesti. [6.]

4.1.1 Point-to-Point-protokolla

PPP-protokollaa käytetään muodostamaan suora yhteys eri verkkolaitteiden välillä. Ensisijaisesti sen käyttökohde on puhelinverkko- sekä modeemiyhteyksissä, mutta myös laajakaistayhteyksissä (PPPoE).

PPP-protokolla koostuu seuraavista tekijöistä:

- Toimii 2. kerroksen siirtoprotokollana synkronisten ja asynkronisten verkkojen yli.
- Tarjoaa tuen dynaamisille IP-osoitteille.
- Toimii usean eri verkkotason protokollan kanssa (esim. IP, IPX, AppleTalk).

- Käyttää FCS-virheentunnistusmenetelmää eli tunnistaa, jos jossain kehyksessä on virhe.

- Hyödyntää LCP-protokollaa, joka luo, konfiguroi ja testaa yhteyden sekä tunnistaa verkkosilmukan eli havaitsee silmukat jotka kiertää verkkoa loputtomasti virheellisen verkon takia.

- Hyödyntää NCP-protokollaa eri verkkoprotokollien konfigurointiin.

Point-to-Point-protokollan kapselointi on suunniteltu mahdollisimman tehokkaaksi, ja näin ollen pyritty minimoimaan hukkakuorman osuus tiedonsiirrossa. Kuten aiemmin esitetyssä luettelossa todetaan, PPP-protokolla tukee useita eri verkkoprotokollia saman datalinkin yli. [7.]

4.1.2 LCP-protokolla

LCP-protokolla on osa PPP-protokollaa, ja sen tehtävänä on luoda, konfigureida sekä testata yhteyden toimivuus. LCP-protokollan toiminta perustuu pakettien lähettämiseen ja vastaanottamiseen. Näin ollen voidaan testata esimerkiksi verkon toiminta ja verkkosilmukka. Jos verkossa havaitaan loputtomasti kiertävä silmukka, on todennäköistä, että verkon rakenne on virheellinen.

LCP-ptotokollan toiminnallinen sisältö perustuu seuraaviin tekijöihin:

- verkon laitteiden tunnistaminen sekä niiden mahdollinen hyväksyminen tai hylkääminen

- hyväksyttävän pakettikoon määrittäminen

- virheiden etsintä

- vastinpäiden käyttämän autentikointimetodin päättäminen

- mahdollisten virhekohtien sulkeminen verkon ulkopuolelle.

PPP-protokollan kannalta LCP-protokolla on kriittinen, koska ilman LCP-protokollan antamaa hyväksyntää verkon käytölle ei tietoa voida siirtää PPP-protokollaa käyttävässä verkossa. [8.]

4.1.3 NCP-protokolla

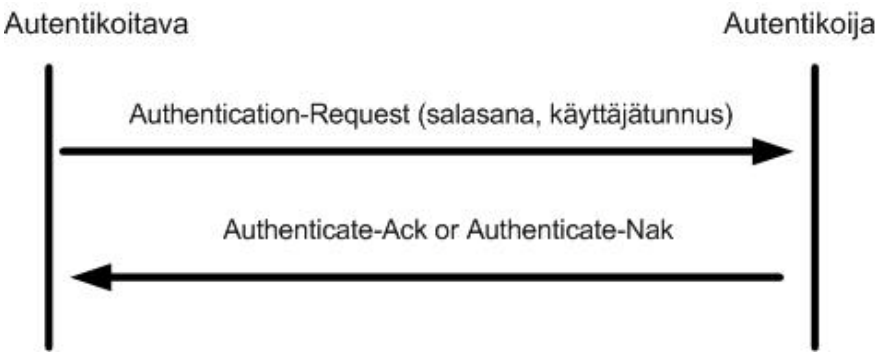
PPP-yhteyksien protokollien konfigurointi saattaa muodostua ongelmalliseksi, mutta sitä varten on kehitetty oma protokollansa, joka kykenee automaattisesti suorittamaan eri verkkoprotokollien konfiguroinnin. Tämä protokolla on NCP-protokollaperhe, joka sisältyy LCP:n tavoin PPP-protokollaan.

Ennen kuin NCP-protokolla kykenee konfiguroimaan verkon asetuksia, täytyy LCP-protokollan suorittaa verkon tarkistus sekä määrittää perusasetukset eri verkkolaitteille ja niiden väliselle yhteydelle. [8.]

4.2 PAP-protokolla

PAP-protokolla, joka toimii PPP-protokollan päällä, on salasanaan perustuva yksinkertainen käyttöoikeuden tunnistusprotokolla, joka perustuu salasanan ja käyttäjätunnistuksen siirtämiseen palvelimelle selkokielisessä muodossa. Kyseisessä protokollassa kirjautumisyritysten määrää ei ole rajoitettu mitenkään, joten toiminta voi jatkua niin kauan, kunnes salasana/käyttäjätunnus osuu oikeaan tai yhteys katkeaa. Koska kyseessä on salaamattomaan tekstiin sekä rajoittamattomiin tiedonsyöttökertoihin perustuva autentikointimenetelmä, ei sitä voida pitää nykystandardien mukaan millään muotoa luotettavana. [9.]

Oheisessa kuvassa esitettynä PAP-autentikoinnin toiminta:



Kuva 7. PAP-autentikointiprotokollan toiminta

PAP-protokollan pohjalta on kehitetty CHAP-protokollaan perustuva tehokkaampi autentikointimenetelmä, joka esitellään seuraavassa kappaleessa.

4.3 CHAP-protokolla

CHAP-protokolla on kehitetty PAP-protokollan pohjalta ja sen toiminta perustuu haaste/vaste-menetelmää käyttävään autentikointiin.

CHAP-autentikointi on huomattavasti varmempi kuin aiemmin esiteltu PAP-autentikointi, ja sitä käytetään yhteyden muodostamisen yhteydessä. CHAP-autentikointi perustuu yhteydenoton, sekä itse yhteyden aikana tehtäviin 3-osaisiin varmistuksiin, jossa varmistetaan yhteyden toisen pään ”henkilöllisyys”. [10.]

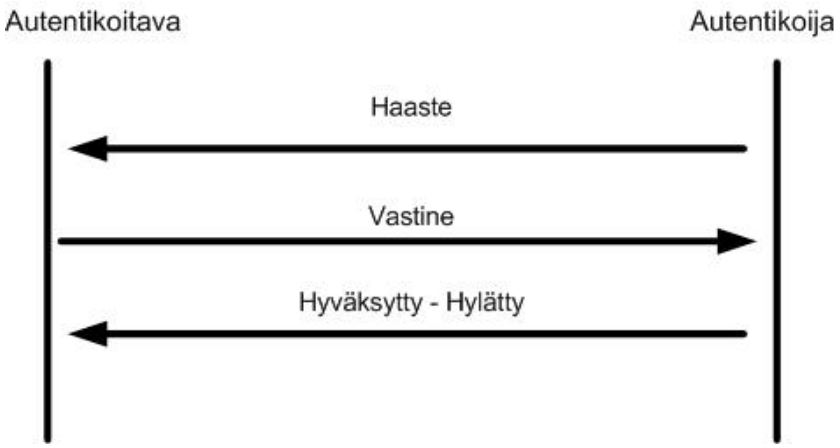
Toiminta perustuu seuraaviin vaiheisiin:

1. Yhteydenoton jälkeen autentikoija lähettää yhteydenottajalle ”haasteen”.

2. Yhteydenottaja lähettää takaisin yksisuuntaisen tiiviste-funktiolla muodostetun vasteen.

3. Autentikoija tarkistaa vasteen ja vertaa sitä omaan hash-funktiolla sekoitetuun odotettuun vasteeseen. Jos arvot vastaavat toisiaan, autentikointi on onnistunut, jos puolestaan eivät, yhteys katkaistaan.

4. Määrätyin väliajoin autentikoija lähettää uuden haasteen yhteydenottajalle.



Kuva 8. CHAP-autentikointiprotokollan toiminta

4.4 EAP-protokolla

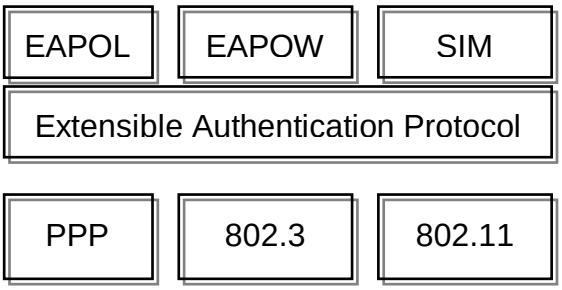
PPP-protokollassa käytettävistä autentikointimenetelmistä kaikkein pisimmälle viety on EAP-protokolla, joka mahdollistaa erilaisten tunnistusmekanismien käytön, eikä näin ollen sidottu vain yhteen mekanismiin. EAP-protokollan suurin vahvuus on sen laajennettavuus. Alun perin kyseinen protokolla on määritelty käyttämään kolmea eri autentikointimetodia, mutta nykyään käytössä on jo kymmeniä erilaisia tapoja suorittaa autentikointi.

Edellä esitellyissä autentikointimalleissa toiminta perustuu vain ennalta määräyttyihin autentikointimenetelmiin, mutta EAP-protokolla tarjoaa huomattavasti laajemman autentikointimenetelmien joukon, jolloin sen tietoturva myös on aivan eri tasolla edellä mainittuihin protokolliin verrattuna. EAP-protokolla ei itsessään tarjoa mitään suoraa autentikointimenetelmää, mutta se tarjoaa optimoidun kuljetusalustan valitulle tunnistetoteutukselle, joka on valittu käytettäväksi. Tästä esimerkkinä tuki RADIUS-protokollalle, jolla käyttäjän autentikointi voidaan toteuttaa.

4.4.1 802.1x

IEEE:n 802.1x-standardi, eli porttikohtainen autentikointi, perustuu EAP-protokollaan, joka tarjoaa laajan ja optimoidun alustan eri autentikointimekanismeille. Vaikka EAP kehitettiin alun perin käytettäväksi PPP-protokollan yhteydessä, on sen laajennettavuus mahdollistanut käytön myös 802.3-standardia tukevissa lähiverkoissa sekä 802.11 langattomissa verkkoratkaisuissa. Tämän myötä se on myös nykypäivän vaatimukset huomioiden erittäin pätevä ratkaisu autentikoinnin toteutuksessa. Se tarjoaa yksinkertaisen ja tehokkaan kuljetustavan EAP-sanomille kaikissa 802.x-pohjaisissa lähiverkoissa.

EAP-autentikointimenetelmä voidaan valita käytettävän verkon mukaan, jolloin sen tehokkuus kyetään optimoimaan. 802.3-standardin mukaisissa lähiverkoissa käytetään yleisesti EAPOL-paketoinititekniikkaa, jolla viestit kuljetetaan autentikointipalvelimelle, joka on tässä tapauksessa RADIUS. Langattomissa verkkoratkaisuissa käytössä on vastaavalla periaatteella toimiva EAPOW (over WLAN). Lisäksi EAP-standardi tarjoaa omat tunnistesovelluksensa ja viestinkuljeturatkaisut mobiileille tietoliikenneratkaisuille jotka toimivat matkapuhelinverkoissa. [11.]



Kuva 9. EAP-arkkitehtuuri

4.4.2 802.1x ja EAP:n toiminta

EAP-arkkitehtuuri muodostuu kolmesta tekijästä. Ne ovat yhteydenottajan päätelaite (Supplicant), verkon reunalla oleva autentikoija (Authenticator) sekä tunnistuspalvelin, johon käyttöön tässä työssä on valittu RADIUS-palvelin. Tunnistuspalvelimelle tallennetaan yhteiseen tietokantaan käyttäjätilit sekä niiden sisältämät autentikointitiedot. RADIUS-palvelimen toiminta esitellään tarkemmin tämän työn kappaleessa 6.

EAP-protokollaan perustuvan käyttäjätunnistuksen tapahtumaketju etenee seuraavasti:

- Lähiverkoissa tunnistetaan kiinteä portti, josta liittymistä yritetään ja langattomissa verkoissa tunnistetaan liittymistä yrittävän päätelaitteen MAC-osoite.

- EAP-keskustelu aloitetaan liittymistä anovan käyttäjän lähettämällä EAPOL-Start-sanomalla, johon autentikoija reagoi kysymällä tunnistetietoja.

- Liittymistä yrittävä käyttäjä antaa tunnuksen ja salasanan. Tässä vaiheessa salasanaa ei lähetetä autentikoijalle suoraan, vaan se tiivistetään ja lähetetään yhteyspisteeseen. Yhteyspiste tarkistaa tiivisteen ja tarkistaa pitääkö kirjautumista yrittävä käyttäjä tunnistaa. Tämän jälkeen EAP-sanoma siirtyy autentikoijalle, joka muuttaa sanoman RADIUS-pyynnöksi ja lähettää sen eteenpäin RADIUS-attribuuttina. Lisäksi sanomaan lisätään MD5-tyyppinen haaste (Challenge).

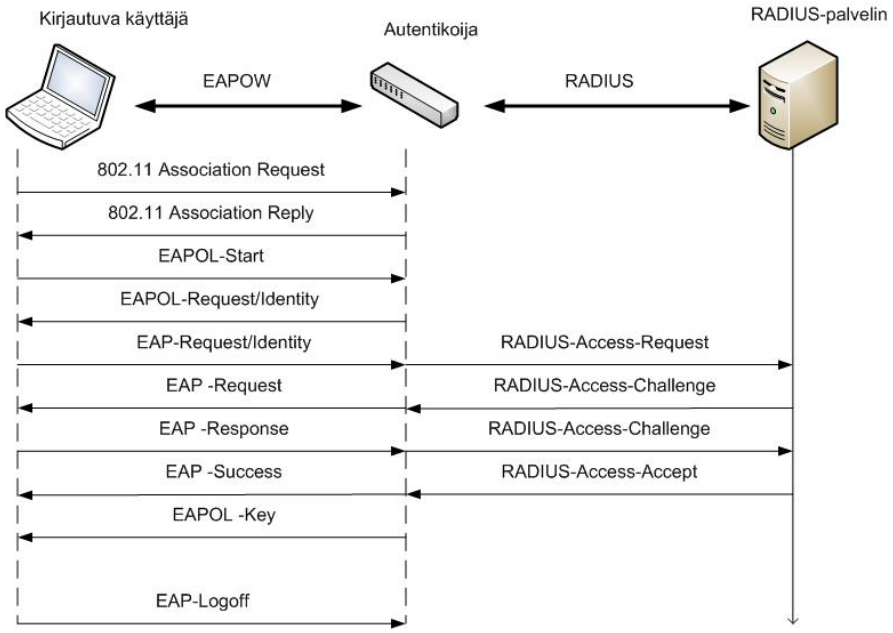
- RADIUS vastaa viestiin haastepaketilla, joka sisältää satunnaisen haasteen sekä salatun MD5-haasteen. Haaste välitetään kirjautumista yrittävälle käyttäjälle EAP:n pyynnöstä.

- Käyttäjän päätelaite lukee annetun salasanan ja salakirjoittaa saadun haastejonon. Lopputulos lähetetään takaisin EAP-vasteessa, joka jälleen muutetaan RADIUS-pyynnöksi.

- RADIUS salaa lähettämänsä haasteen paikallisesi käyttäjän antamalla salasanalla ja vertaa tulosta saatuun sanomaan. Jos salatut haasteet täsmäävät, voidaan käyttäjä liittää verkkoon. Tällöin RADIUS lähettää positiivisen RADIUS-Access-Accept-sanoman, jonka autentikoija muuttaa EAP-Success-sanomaksi. Tämän myötä RADIUS lähettää myös ko. Istunnon WEP-avaimen, jonka yhteyspiste tallentaa ja lähettää eteenpäin käyttäjlle.

- WEP-avainta voidaan vaihtaa tasaisin väliajoin, jolloin yhteyspiste välittää sen aina uudestaa käyttäjälle.

- Istunnon päätyttyä käyttäjän päätelaite lähettää EAP-logoff-sanoman yhteyspisteelle, jolloin ko. käyttäjän päätelaite poistetaan verkosta. [11.]



Kuva 10. EAP-sanomaliikenne

5 AUTENTIKOINTIPROTOKOLLAT

Käyttäjän autentikointi suoritetaan käyttämällä AAA-protokollaa, joka on kehys mihin käyttäjätunnistus eri vaiheineen perustuu. Prosessi sisältää kolme eri tekijää, eli käyttäjän todentamisen (Authentication), valtuutuksen (Autho-

rization) sekä tilastoinnin (Accounting). Nämä kolme eri tekijää sisällytetään yleensä yhden AAA-palvelimen, kuten esim. RADIUS, alle, jolloin niiden toiminta voidaan asettaa yhdenmukaisesti ja näin ollen minimoida ns. heikot kohdat. [12. 115-117]

Kokonaisuudessaan AAA-protokollaan perustuva käyttäjän autentikointi on erittäin keskeisessä asemassa nykyisessä jokapäiväisessä tietoliikenteessä ja tietoverkkojen käytössä etenkin yritysmaailmassa, jossa jaettava tieto halutaan kohdentaa vain halutuille henkilöille. Yksinkertaistettuna kyseinen protokolla tunnistaa käyttäjän ja määrittelee, mitä kyseinen käyttäjä saa verkon sisällä tehdä esimerkiksi eri verkkolaitteille, eli antaa oikeudet sekä kerää tietoja käyttäjän toiminnasta ja suorittamista toimenpiteistä. Periaatteessa AAA-protokollan toiminta voidaan sisällyttää seuraaviin yksinkertaisiin kysymyksiin:

- Kuka olet?

- Mitä palveluita ja oikeuksia sinulle saa antaa?

- Mitä teit oikeuksillasi?

AAA-teknologia voidaan toteuttaa useallakin eri tavalla, joista yleisimmät järjestelmät ovat RADIUS sekä TACACS. Tässä kyseisessä työssä tutkitaan lähemmin RADIUS-palvelimella suoritettavaa käyttäjän autentikointia, joka on siis verkossa ulkopuolinen autentikointipalvelin, joka suorittaa käyttäjän todennuksen, valtuutuksen sekä tilastoinnin. Sekä RADIUS että TACACS tukevat useita eri valmistajien verkkolaitteita, mutta esim. TACACS, joka on CISCO Systemsin kehittämä, toimii kaikkein parhaiten CISCON verkkolaitteilla, jotka ovat markkinajohtajan asemassa. Valinta RADIUS-palvelimeen kohdistuu sen laajan käyttäjäkunnan, ja sen tarjoaman dokumentaation, muokattavuuden sekä vapaan lähdekoodin ohjelmiston takia.

5.1 Yleistä käyttäjätunnistuksesta

Käyttäjätunnistus mielletään yleisesti siihen, että verkkoon kirjaudutaan jollain ennalta määrätyllä käyttäjätunnuksen ja salasanan yhdistelmällä. Kuitenkaan tämä ei käytännössä riitä silloin kun kyseessä on verkko, jossa on monia käyttäjiä, jotka voivat esimerkiksi hallita eri verkkolaitteita sekä suorittaa tiettyjä toimenpiteitä tai jos verkossa liikkuu tietoa, johon ei kaikkien käyttäjien haluta pääsevän käsiksi. Tällöin verkon sisäistä liikennettä tulee rajata

tiettyjen tunniste-elementtien mukaan niin, että vain tietyillä annetuilla oikeuksilla saa tehdä tiettyjä toimenpiteitä verkon eri laitteille tai tietyillä oikeuksilla pääsee vain haluttuun jaettavaan tietoon käsiksi. Käyttäjän tunnistukseen käytettäviä malleja esitellään myöhemmin tarkemmin tässä kappaleessa. Yksinkertaistettuna kuitenkin voidaan todeta että tunnistukseen käytettävät mallit voidaan jakaa kolmeen eri luokkaan toimintatapojen mukaan:

- käyttäjän tiedossa olevaan salasanaan pohjautuva tunnistus

- hallussa olevaan esineeseen perustuva tunnistus

- biometrinen tunnistus.

Lisäksi näitä vaihtoehtoja voidaan yhdistellä, jolloin saadaan luotua entistä vahvempi ja turvallisempi käyttäjäntunnistus. Kuitenkin näistä kolmesta menetelmästä ylivoimaisesti käytetyin on salasanaan perustuva tunnistus, koska muita vaihtoehtoja pidetään liian monimutkaisina käyttää. Tulevaisuudessa varmasti kuitenkin muutkin mallit yleistyvät huomattavasti, koska pelkkä käyttäjätunnus ja salasana yhdistelmän riittävyyteen ei välttämättä enää pystytä pelkästään luottamaan.

Kokonaisuuden kannalta tulee tärkeäksi tekijäksi tiedon tallentaminen ja varastointi, jotta voidaan jälkikäteen tarvittaessa kohdistaa kaikki verkon sisällä tehdyt toimenpiteet tiettyihin käyttäjiin. [13. 1-5]

5.2 Autentikointi (Authentication)

Käyttäjän tunnistus, eli autentikointi tarkoittaa palvelua, jolla tunnistetaan verkkoon kirjautuneen henkilön tai laitteen identiteetti sen MAC-osoitteen perusteella. Tällöin varmistutaan siitä, että kirjautuva käyttäjä on juurikin se, joka väittää olevansa. Yleisesti autentikointi suoritetaan jaetulla salaisuudella luotettavan kolmannen osapuolen autentikointijärjeselmän toimesta.

Autentikoinnilla pystytään myös rajaamaan verkon resursseja eri käyttäjien kesken, eli vältytään jakamasta yrityksen verkon resursseja sellaisille henkilöille joille ne eivät kuulu. Tästä käy hyvänä käytännön esimerkkinä yritysverkon vierailijatunnukset tai yrityksen sisäisten organisaatioiden erilaiset verkkotarpeet. Varmasti yleisin autentikointimalli on käyttäjän syöttämä käyttäjätunnuksen ja salasanan yhdistelmä. Tämä käyttäjän tunnistus ei kuiten-

kaan ole kaikissa tapauksissa riittävä, joten vaihtoehtoisia sekä paremman suojauksen tarjoavia menetelmiä on kehitetty useita. [13. 1-5]

5.3 Valtuutus (Authorisation)

Valtuutus, eli AAA-protokollan toinen ”A” tarkoittaa käyttäjäoikeuksien jakamista verkossa, eli käyttäjän valtuuttamista tiettyihin toimenpiteisiin tai pääsyä verkon tiettyihin alueisiin ja tietoihin. Valtuutus suoritetaan perustuen autentikointiin, joka noudattaa ennalta määrättyä protokollaa, eli tietyillä käyttäjillä on omat tietyt valtuudet tehdä erilaisia toimenpiteitä verkossa. Valtuutus suoritetaan autentikoinnin jälkeen, eli kun käyttäjä on onnistuneesti kirjautunut verkkoon ja käyttäjä on autentikointipalvelimen toimesta tunnistettu juuri siksi käyttäjäksi, jolla on oikeudet kirjautua verkkoon.

Tällaisia tiettyjä valtuuksia vaativia toimenpiteitä voivat olla esimerkiksi eri verkkolaitteiden asetusten muokkaaminen tai tietyt korjaustoimenpiteet, eri verkon osiin pääseminen tai yksinkertaisimmillaan tiettyihin kansioihin ja tiedostoihin pääseminen tai pääsyn estäminen.

Valtuutuksella voidaan esimerkiksi jakaa eri kansioita eri yritysten eri organisaatioiden sekä niiden työntekijöiden kesken eikä näin ollen tarvitse pelätä väärien tietojen joutuvan niiden henkilöiden tietoon, joiden ei kyseiseen tietoon kuulu päästä käsiksi.

Lisäksi valtuutuksella voidaan jakaa oikeuksia päästä eri verkkolaitteisiin sekä niiden asetuksiin käsiksi. Tämä on hyödyllistä esimerkiksi silloin, kun halutaan antaa esim. tietylle henkilölle oikeus päästä muuttamaan jonkin yhden verkkolaitteen asetuksia, mutta samalle henkilölle ei kuitenkaan haluta antaa koko verkon hallintaa kattavia oikeuksia. [12. 115-117]

Valtuutuksella kyetään myös verkonvalvojan toimesta määrittämään käyttäjän protokollat, joita käyttäjän halutaan käyttävän verkossa.

5.4 Tilastointi (Accounting)

Alunperin tiedon säilytykseen ei kiinnitetty eri protokollissa juurikaan huomiota, vaan pääpaino oli ainoastaan käyttäjän tunnistamisessa ja valtuutuksessa, ja näin ollen esimerkiksi RADIUS-protokolla ei alunperin tukenut ollenkaan tilastointia.

Tilastointi suoritetaan sen jälkeen, kun käyttäjän valtuutus on suoritettu, eli ollaan pystytty todentamaan käyttäjän henkilöllisyys sekä antamaan käyttäjälle sille kuuluvat oikeudet.

Tilastoinnilla voidaan kerätä käyttäjästä sekä sen verkossa suorittamista toimenpiteistä useita erilaisia tietoja, joita voidaan käyttää vakavimmassa tapauksessa jopa todisteena oikeudessa mahdollisissa väärinkäyttötapauksissa tai tietomurroissa. Tämän mahdollistaa se, että käyttäjästä voidaan mitata esimerkiksi yhteyden kestoaika, lähetetyn ja vastaanotetun datan määrä sekä kirjautumistiedot eri verkon laitteille.

Tilastointi mahdollistaa myös verkossa suoritettujen toimenpiteiden valvonnan, koska tällöin kyetään tarkasti määrittelemään verkkoon ja sen laitteiden asetuksiin tehdyt muutokset sekä mahdollisissa ongelmatilanteissa jäljittämään ongelman alullepanija.

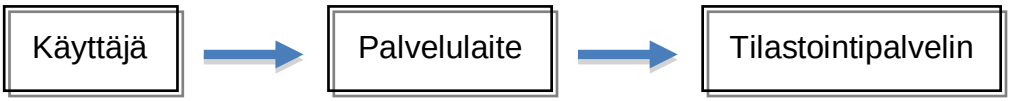
Lisäksi tilastoinnin avulla pystytään keräämään esimerkiksi tietoja laskutusta varten.

Tilastoinnin suorittaa valittu verkossa toimiva autentikointipalvelin, eli tässä tapauksessa RADIUS-palvelin. [12. 115-117]

Käyttäjätilastoiden keräyksen yleinen malli koostuu kolmesta eri tekijästä, jotka ovat:

- käyttäjä
- palvelulaite
- autentikointipalvelin, joka toimii myös tilastointipalvelimena.

Käytännössä tilastointi etenee niin, että palvelulaite tarjoaa käyttäjälle sen haluaman/tarvitseman palvelun, jonka jälkeen se lähettää tilastointipalvelimelle tiedot käyttäjän aloittaessa sekä lopettaessa halutun palvelun käytön. Lisäksi tilastotietoa voidaan kerätä myös käytön aikana halutulla tavalla. Jos tilastoinnin sekä sen myötä verkonvalvonnan ei tarvitse toimia ”aktiivisena”, voidaan tilastoja kerätä ns. välivarastoon ja lähettää tilastointipalvelimelle kerralla suurempi määrä tilastoitua tietoa. [14.]



Kuva 11. Käyttötilastojen kerääminen

5.5 Autentikoinnissa käytettävät ratkaisut

Kuten aiemmissa kappaleissa on jo todettu, ylivoimaisesti yleisin käyttäjän tunnistusmenetelmä on käyttää yksinkertaista käyttäjätunnuksen ja salasanan yhdistelmää. Tämä ratkaisu ei kuitenkaan täytä nykyisiä tietoturvavaatimuksia, ja tämän myötä on markkinoille kehitetty useita vaihtoehtoisia ratkaisuita, jotka antavat huomattavasti luotettavamman lähtökohdan käyttäjän kirjautumiselle verkkoon. Osa näistä ratkaisuista kuitenkin aiheuttavat mahdollisia lisäkustannuksia aiheuttavia päivityksiä jo olemassa oleviin järjestelmiin, mutta niistä saatava hyöty kuitenkin yleisesti siinä määrin suuri, että kyseisiä ratkaisuita voidaan pitää erittäin varteenotettavina. Seuraavaksi esitellään yleisimmin käytössä olevat autentikointiratkaisut.

5.5.1 Käyttäjätunnistus salasanan perusteella

Tiettyyn salasanaan perustuva käyttäjätunnistus on tuttua jokapäiväisessä elämässä esimerkiksi verkkokäyttöisiin sähköpostipalvelimiin kirjautumisen muodossa. Yksinkertaisesti ilmaistuna salasana on yleisesti käyttäjän itsensä määrittämä tietyn mittainen ja tiettyjä merkkejä sisältävä tunnus, jolla kirjaudutaan verkkoon. Verkon valvoja kykenee määrittämään tietyt ehdot, jotka salasanan tulee täyttää, mutta silti ongelmaksi muodostuu liian usein käyttäjän valitsema liian yksinkertainen salasana. Lisäksi salasana saattaa liikkua verkossa salaamattomana, on siihen sopivilla taidoilla ja sopivissa olosuhteissa erittäin helppoa päästä käsiksi väärin perustein ja näin ollen aiheuttaa selkeän uhan tietoturvalle. Myös käyttäjän antamia komentoja keräävät Keylogger-ohjelmistot aiheuttavat tässä tapauksessa uhan tietoturvalle. Keylogger perustuu näppäinkomentojen tallentamiseen, jolloin hyökkääjä saa kaapattua esim. käyttäjän antamat tunnukset ja salasanat. [15.]

5.5.2 Esinepohjainen käyttäjätunnistus

Esinepohjainen tunnistus perustuu hyvin useasti käyttäjän hallussa olevaan esineeseen, joka tarjoaa muuttuvan sekä kertakäyttöisen salasanan jokaiselle verkkoon kirjautumiselle. Kyseinen malli on yleensä yhdistetty johonkin pysyvään käyttäjätunnukseen, eli ainoastaan salasana muuttuu jokaisella

kirjautumiskerralla. Kyseiseen malliin on kehitetty erilaisia toteutusratkaisuita, joita voivat olla esimerkiksi pankkien suosimat tunnuslistat, joista valitaan aina tiettyä numeroa vastaava koodi, tai erilaisten tietoturvayritysten tarjoama digitaalinen laite, joka generoi tietyllä algoritmillä jokaiselle kirjautumiskerralle uuden salasanan. Kyseinen malli tarjoaa huomattavasti aukottomamman autentikoinnin kuin pelkkä käyttäjätunnuksen ja salasanan yhdistelmä, koska kyseistä esineeseen pohjautuvaa salasanaa on mahdoton väärentää. Ainoa tapa murtaa kyseinen autentikointi on tilanne, jossa salasanan tuottava esine joutuu väärän käyttäjän käsiin, jolloin tietomurtoon riittää ainoastaan pysyvän käyttäjätunnuksen selvittäminen.

Kyseiseen esinepohjaiseen autentikointiin nykyisin yritysmarkkinoilla on otettu käyttöön matkapuhelinta hyväksikäyttävä malli, jossa käyttäjän matkapuhelimeen asennetaan ohjelmisto, joka luo uuden järjestelmään syötettävän salasanan jokaiselle kirjautumiskerralle. Lisäksi voidaan käyttää järjestelmää, jossa käyttäjä tilaa uuden kirjautumisen mahdollistavan salasana tekstiviestillä. Kyseinen ratkaisu tarjoaa siinä mielessä helpon vaihtoehdon esinepohjaiselle autentikoinnille, että tällöin käyttäjän ei tarvitse kuljettaa matkapuhelimen lisäksi mitään muuta autentikointiin tarvittavaa esinettä, kuten esim. SecurID-korttia tai muuta pientä mukana kulkevaa laitetta, joka normaalisti suorittaisi salasanan generoinnin. [16.]

5.5.3 Biometrinen käyttäjätunnistus

Kaikkein kehittynein ja tämän myötä myös luotettavin autentikointimalli tähän mennessä esitetyistä on biometrinen käyttäjätunnistus. Biometrinen autentikointi perustuu johonkin valittuun tunnistettavan henkilön fyysiseen ominaisuuteen tai piirteeseen, joka voi olla esimerkiksi jokin tietty ruumiin rakenteellinen ominaisuus. Tällöin tunnistaminen toimii niin, että tulosta verrataan aiemmin todennettuun tietoon. Jos vertailtava kohde ja sen identiteetti on riittävän tarkasti samanlainen vertailtavan kohteen kanssa, autentikointi onnistuu.

Biometrinen autentikointi asettaa tiettyjä ehtoja autentikointiin valittavalle piirteelle:

- piirteen pitää olla selkeästi henkilökohtainen.
- piirteen pitää olla tarpeeksi selkeästi tunnistettavissa.

- piirteen tulee olla pysyvä.
- piirre ei saa olla alttiina muutoksille.

Nämä ehdot huomioon ottaen, sekä nykyisen tekniikan puitteissa järkevimmin toteutettavissa olevia tunnistuselementtejä ovat sormenjälki sekä silmän iirikseen perustuva autentikointi. Kyseinen autentikointimalli on kuitenkin haasteellinen sikäli, että se vaatii käyttöönsä jonkin tunnistamisen suorittavan teknisen apuvälineen, jotka eivät vielä ole kovin yleisiä ja ovat hankintakustannuksiltaan vielä melko kalliita. Tosin kannettavien tietokoneiden valmistajat tarjoavat jo useissa malleissaan sormenjälkitunnistuksen mahdollistavan sormenjälkiskannerin, joten sen käyttäminen tunnistuksen suorittamisessa on siltä osin mahdollista. Ainoastaan se asettaa ehdoksi, että organisaation sisällä kaikilla käyttäjillä tulee olla hallussaan tietokone, josta tämä sormenjälkiskanneri löytyy.

Vaikka biometrinen tunnistus on esitellyistä vaihtoehdoista kaikkein aukottominen, ei sekään silti tarjoa 100%:in luotettavuutta. Mahdollisuutena on esimerkiksi sormenjälkien kopioiminen tai vastaava tunnistettavan piirteen väärinkäyttö. Tämän takia varmin keino on yhdistää esiteltyjä malleja niin, jolloin autentikoinnin vahvuutta voidaan kasvattaa. Tällaisesta yhdistelmästä käy hyvänä esimerkkinä sormenpäätunniste, joka tunnistaa myös sormen lämpötilan tai pulssin. Tällöin kyetään lisäämään jälleen autentikoinnin luotettavuutta. [17.]

5.5.4 Autentikointimallien yhdistäminen

Koska esitellyistä autentikointimalleista mikään ei yksinään tarjoa 100%:n aukotonta tietosuojaa, voidaan tapoja yhdistellä ja näin ollen luoda vahva autentikointi. Vahvan autentikoinnin yleisin tapaus on yhdistää kaksi erilaista tapaa suorittaa käyttäjän tunnistus. Näistä yleisin on käyttäjätunnuksen sekä esineeseen perustuvan muuttuvan salasanan yhdistäminen. Tämä malli on käytännössä vielä nykyisessä yritysmaailmassa peruskäytössä riittävä.

Yksinkertaistettuna tunnistus voidaan todeta vahvaksi, jos

- se sisältää jotain minkä käyttäjä tietää (käyttäjätunnus).
- se sisältää jotain mitä käyttäjällä on hallussaan (muuttuva salasana).
- se sisältää jotain mitä käyttäjä on (esim. sormenjälki).

Teknisesti näiden tekijöiden toteuttaminen on täysin mahdollista ja näin ollen myös nykyään hyvin yleistä. Kun käyttäjän autentikointitekniikka on selvillä, voidaan suorittaa myös valtuutus sekä käyttäjän suorittaminen toimintojen tilastointi, Tähän käyttöön valitaan erillinen autentikointipalvelin, joka on tässä työssä valittu RADIUS. [18.]

6 RADIUS

Tässä kappaleessa esitellään työn toteutukseen valittu RADIUS-palvelin ja sen toiminta AAA-järjestelmässä. Aiemmissa kappaleissa on jo hieman sivuttu RADIUS-palvelimen toimintaa, mutta tässä kappaleessa esitellään autentikointipalvelimen toiminta sekä vaihtoehdot yksityiskohtaisesti.

6.1 Yleisesittely

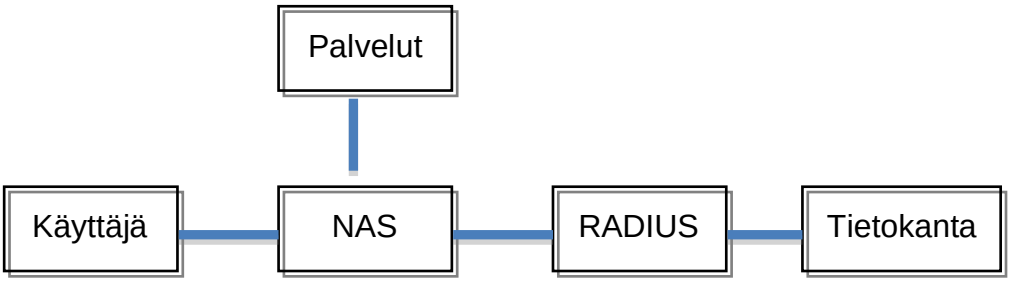
RADIUS mahdollistaa verkossa käytettävän ja aikaisemmin esitellyn AAA-mallin toteutuksen, eli käyttäjän tunnistuksen, valtuutuksen sekä käyttäjätietojen tilastoinnin.

Alun perin RADIUS kehitettiin Livingston-yhtiön toimesta sisäänsoittopalveluihin suorittamaan käyttäjän tunnistus. Tässä vaiheessa oli kehitteillä myös muita vastaavantyyppiseen käyttötarkoitukseen suuntautuvia protokollia, mutta ajan saatossa RADIUS on kohonnut suosituimmaksi ratkaisuksi verkon AAA-toteutuksessa.

RADIUS ja sen toiminta on määritelty kahdessa eri RFC-standardissa, joista RFC 2868 määrittelee käyttäjän tunnistamisen sekä valtuutuksen ja RFC 2867 käyttäjätietojen tilastoinnin. [13. 15-17]

AAA-palvelin, joka on toteutettu RADIUS-protokollalla, mahdollistaa esimerkiksi yrityksen tietoverkossa hyvin tehokkaan ja toimivan käyttäjien autentikointijärjestelmän. RADIUS:ta käytetään yleisesti suljetuissa verkoissa, jollainen esimerkiksi yrityksen sisäinen verkko, tai sen sisäinen virtuaalinen lähiverkko on, jolloin verkkoon liittyminen tapahtuu määriteltyjen liityntäpidteiden, NAS:ien kautta. Koska RADIUS mahdollistaa autentikointitoimintojen keskittämisen yhdelle, tai laajemmassa verkossa muutamalle autentikointipalvelimelle, niiden ylläpito on helppoa eikä vaadi suuria henkilöresursseja ylläpitäjältä. Palvelimen pääasiallinen tehtävä on siis autentikoida käyttäjä ja jakaa käyttäjälle ennalta määrätyt oikeudet suorittaa verkossa toimenpiteitä,

joihin käyttäjällä on oikeus sekä päästä muokkaamaan tietoja jaettujen oikeuksiensa mukaan. Toinen palvelimen tehtävä on kerätä käyttäjän suorittamista toimenpiteistä tietoa, jolla ylläpitäjä voi jälkikäteen tutkia verkossa tapahtuvaa liikennettä sekä suoritettuja toimenpiteitä. [19.]



Kuva 12. RADIUS-palvelinta käyttävään verkkoon liittyminen

RADIUS-protokollan keskeiset ominaisuudet voidaan määritellä seuraavanlaiseisti:

- asiakas-palvelinmalli
- verkkoliikenteen turvaaminen
- toimiva autentikointi
- laajennettavuus.

Näiden lisäksi RADIUS tukee lähes kaikkia markkinoilla olevia NAS-palvelimia, joten sen yhteensopivuus tekee sen verkkoon liittämisen mahdollisimman yksinkertaiseksi. Lisäksi RADIUS-protokolla tukee aiemmin esiteltyjä PAP, CHAP sekä EAP-arkkitehtuureja. [19.]

RADIUS siis on asiakas-palvelinmallin mukainen protokolla, jonka asiakkaana toimii käyttäjän verkkoon liityntäpiste NAS. Palvelin vastaanottaa NAS:n lähettämiä autentikointipyyntöjä, joiden perusteella se suorittaa käyttäjän autentikoinnin ennalta annettujen ehtojen mukaan. Jos ehdot täyttyvät, se vastaa NAS:lle, että autentikointi on suoritettu. Autentikoinnin yhteydessä suoritetaan myös käyttäjän valtuutus, jotta käyttäjä pääsee sille osoitetuille alueille verkossa tai käsittelemään sille osoitettuja tietoja. Käyttäjien valtuutus suoritetaan aiemmin mainitun standardin mukaisesti.

Jos verkossa käytetään enemmän kuin yhtä RADIUS-palvelinta, voi se toimia myös välityspalvelimena, jolloin tunnistetieto välitetään toiselle RADIUS-palvelimelle. Välitys voidaan määritellä toteutettavaksi esimerkiksi tiettyjen käyttäjätunnusten ominaisuuksien mukaan. [13. 63-76]

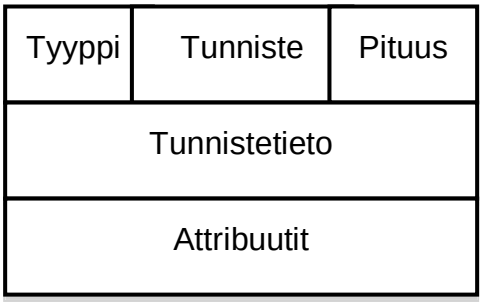
6.2 RADIUS-palvelimen toiminta

Kuten on todettu, palvelimen tehtävänä on suorittaa verkkoon kirjautumista yrittävän käyttäjän tunnistus, valtuuttaa käyttäjä sekä suorittaa verkon käytön tilastointi.

Tunnistusprosessi sisältää kolme eri osapuolta:

- asiakas eli autentikoitava käyttäjä
- NAS-liityntäpiste
- RADIUS-palvelin.

Järjestelmä koostuu siis yhdestä tai useammasta palvelimesta, joka sisältää RADIUS-ohjelmiston sekä niitä käyttävistä käyttäjistä. Käyttäjiksi määritellään yleisesti verkkoon liittymispisteet, jotka käyvät RADIUS-viestien vaihtoa palvelimen kanssa käyttäen UDP porttia 1812. Liityntäpiste kysyy käyttäjältä tunnistetietoa, joka yksinkertaisimmillaan on käyttäjätunnuksen ja salasanan yhdistelmä, jonka jälkeen se välittää saadun tiedon autentikointipalvelimelle, joka suorittaa tarkistuksen ja jos tiedot täsmäävät, suorittaa myös käyttäjän tunnistuksen ja valtuutuksen.



Kuva 13. RADIUS-viestin rakenne

Autentikointipalvelimelle lähetettävä autentikoitava tieto salataan, jotta pystytään minimoimaan riski siitä, että tieto joutuisi salaamattomana väriin käsiin. RADIUS-viestien tyyppikenttä määrittelee viestin tyypin. Tunniste-kentän avulla tunnistetaan toisiinsa liittyvät viestit, pituus-kenttä määrittää viestin pi-

tuuden. Tunnistetieto salaa välitettävän viestin ja salasanan. Attribuutit-kenttä välittä tietoa käyttäjän (NAS) sekä palvelimen välillä [19].

Taulukko 1. RADIUS-viestityypit

Koodi	Tyyppi
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server
13	Status-Client
255	Reserved

6.2.1 Autentikointi ja valtuutus

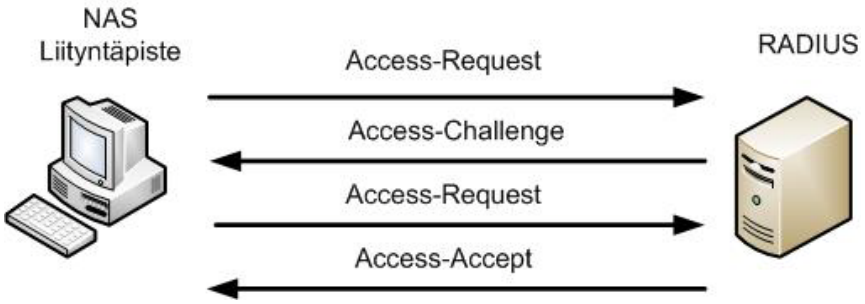
Nyt kun on kerrottiin, millaisia viestityyppejä on käytössä, voimme tarkemmin esitellä niiden toimintaa. Käyttäjän tunnistuksen ja valtuutuksen kannalta tärkeimmät viestit AAA-mallissa ovat *Access-Request*, *Access-Accept*, *Access-Reject* sekä *Access-Challenge*.

Autentikointiprosessi lähtee liikkeelle autentikoitavan käyttäjän yrittäessä liityntäpisteen kautta kirjautumista verkkoon. Tällöin liityntäpiste (NAS) lähettää RADIUS-palvelimelle *Access-Request*-paketin, jolla pyydetään palvelinta suorittamaan autentikoiti. Tyyppikentän arvona tässä paketissa tulee olla 1. Kyseinen paketti sisältää kaikki autentikoinnin suorittamiseksi vaadittavat arvot, jolloin RADIUS pystyy määrittelemään, onko käyttäjä oikeutettu kirjautumaan verkkoon. Lähetettävän paketin tulee sisältää myös käyttäjätietojen lisäksi laitteen IP-osoitetiedot sekä verkkolaitteen tiedot, joista kirjautumista yritetään. Salasana salataan käyttämällä MD5-salausta.

Jos käyttäjä tunnistetaan, lähetetään takaisin paketti *Access-accept,* jolla käyttäjä hyväksytään, tai jos käyttäjän tunnistetietoja ei hyväksytä, lähetetään *Access-Reject* viesti, jolla kirjautumisyritys hylätään. *Access-Accept*-viestin tyyppikentän arvo on 2 ja *Access-Reject*-kentän 3.

Access-Reject-paketilla pystytään myös hallitsemaan käyttäjän toimintaa vaikka autentikointi sinänsä olisikin onnistunut. Esimerkiksi verkkoon kirjautumisen aikarajan täytyttyä (jos aikaraja on määritelty), voidaan lähettää *Access-Reject*-paketti, jolla kirjautuminen verkkoon katkaistaan.

Mikäli palvelin ei kykene suorittamaan käyttäjän tunnistusta pelkästään Access-Request-viestin sisältämän tiedon perusteella tai halutaan lisätä tiedon luotettavuutta, voidaan käyttäjälle lähettää *Access-Request*-viestin vastaukseksi lisähaaste *Access-Challenge*-viestinä. Kyseisellä viestillä pyydetään kirjautumista yrittävältä käyttäjältä haluttua lisätietoa, jotta voidaan varmentaa käyttäjä tehokkaammin. Kun palvelin on lähettänyt käyttäjälle lisähaasteen, etenee prosessi samalla tavalla kuin jos autentikointiin käytettäisiin vain *Access-Request*-pakettia. [13. 21-23]



Kuva 14. RADIUS-viestiliikenne

Kuten aiemmin jo todettiin, kykenee RADIUS-palvelin myös välittämään autentikointipyyntöjä toiselle RADIUS-palvelimelle, jolloin liikkuminen verkojen välillä on käyttäjän kannalta huomattavasti sulavampaa. Toiminnallisesti kyseinen malli ei eroa käyttäjän havaittavalla tavalla siitä, kuin jos käytössä olisi vain yksi palvelin, joka suorittaa autentikoinnin. Enemmän kuin yhden palvelimen käytössä käyttäjätietokannan ei tarvitse sijaita kuin siinä palvelimessa, joka viimekädessä suorittaa käyttäjän tunnistamisen ja valtuutuksen, eli muut palvelimet ainoastaan välittävät autentikointipyyntöjä. [19.]

6.2.2 Tilastointi

RADIUS-protokollan ensimmäisissä versioissa ei ollut mahdollisuutta käyttäjätietojen tilastointiin ja näin ollen niiden myöhempään tutkimiseen. Jotta verkon ylläpito sekä seuranta helpottuisi, kehitettiin standardiin myöhemmin myös tilastoinnin mahdollisuus.

Tilastointi on verkon valvonnan sekä ylläpidon kannalta erittäin tärkeä ominaisuus, joka korostuu operaattoreiden tarpeissa. Tilastoinnilla kyetään seuraamaan monia erittäin tärkeitä yksityiskohtia, joita käyttäjät verkossa suorittavat. Tällaisia ovat esimerkiksi

- siirretty data

- kirjautumisen aika
- verkon laitteille tehdyt muutokset (jos käyttäjällä on oikeuksia niihin)
- käytettävät osoitteet.

Kyseistä kerättyä dataa voidaan käyttää esimerkiksi operaattoreiden toimesta laskuttamiseen tai verkonvalvojan työkaluna virhetilanteiden selvittämisessä. Tällöin voidaan jäljittää verkkolaitteisiin tehdyt muutokset sekä todentaa johtuuko mahdollinen vikatilanne näistä muutoksista.

Esitellyistä RADIUS-viesteistä, tilastoinnissa käytössä olevia viestejä ovat *Accounting-Request* (Start/Stop) sekä *Accounting-Responce*. Viestin muoto on sinällään samanlainen kuin itse autentikoinnissakin käytettävän viestin.

Tilastointi aloitetaan käyttämällä *Accounting-Request*- (Tyyppikentän arvo 4) viestiä käyttäjän tunnistuksen jälkeen, jonka palvelin kuittaa *Accounting-Response*-viestillä (Tyyppikentän arvo 5). Istunnon päätyttyä toiminto suoritetaan uudelleen, jolloin kerrotaan että kyseinen istunto päättyy sekä kirjataan ylös halutut tiedot istunnosta. [13. 63-76]

Käyttäjätietojen tallennus tietokantaan voidaan toteuttaa teknisesti esimerkiksi käyttämällä MySQL-tietokannan hallintajärjestelmää tai Microsoftin kehittämää Active Directory -ratkaisua.

MySQL on avoimeen lähdekoodiin perustuva tietokannan hallintajärjestelmä, joka mahdollistaa esim. web-palveluiden tietokantojen hallinnan erittäin tehokkaasti. Esimerkkinä tästä voi olla verkkokauppa tms. Sovellus, jossa kerätään tietoja asiakkaista rekisteriin. Tässä esimerkissä tietokantaan tallennetaan myös käyttäjien salasana- ym. kirjautumistiedot, jolloin se on hyvin läheisessä käytössä autentikointipalvelimen kanssa. [22.]

Active Directory on yhtälailla käyttäjien tietoja keräävä keskitetty hakemistopalvelu, joka sisältyy Microsoftin Windows Server -tuotteisiin. Kyseinen palvelu mahdollistaa käyttäjätietojen, verkkoresurssien sekä verkkolaitteiden tietojen keräämisen. Koska kyseessä on Microsoftin Windows ympäristöön sijoittuva tuote, on sen dokumentaatio ja tuki kilpailijoita kehittyneemmällä tasolla, mutta sen muokattavuus sekä sidonnaisuus ainoastaan Windows-ympäristöön ei mahdollista niin suurta vapautta kuin esimerkiksi MySQL.

6.3 RADIUS-palvelimet

Kuten aikaisemmissa kappaleissa jo todettiin, ensimmäisen RADIUS-palvelimen kehitti Livingston-yhtiö, joka kuitenkin päästi palvelimensa heti vapaaseen levitykseen, ja näin ollen siitä on muotoutunut monia eri kehittäjien variaatioita, mutta perusperiaate on kuitenkin pysynyt samana, eli palvelin suorittaa käyttäjän tunnistamisen.

RADIUS-palvelimesta on olemassa sekä maksullisia versioita että ilmaisia vapaan lähdekoodin muunnoksia, jotka kuitenkin tarjoavat samat ominaisuudet kuin maksulliset versiot sekä ovat lisäksi muokattavissa juuri tiettyihin haluttuihin käyttötarkoituksiin. Tässä työssä käsitellään ainoastaan vapaassa levityksessä oleviin RADIUS-palvelin ohjelmistoihin, joista tarkempaan tutkintaan on valittu Open RADIUS sekä FreeRADIUS. Kyseiset ohjelmat mahdollistavat yrityksen tai jopa operaattorin sisäisen verkon käyttäjäautentikoinnin, valtuutuksen sekä tilastoinnin toteutuksen, joten kaupalliset tuotteet voidaan tässä tapauksessa sivuuttaa. Mahdollinen yrityksessä luotava autentikointijärjestelmä tullaan tulevaisuudessa myös toteuttamaan käyttämällä näitä avoimen lähdekoodin ohelmistoja.

6.3.1 FreeRADIUS

FreeRADIUS on vapaan lähdekoodin RADIUS-palvelimista kaikkein laajimmalle levinnyt sekä tällä hetkellä pisimmälle kehitetty kokonaisuus.

FreeRADIUS on edelleen hyvin yhteensopiva esimerkiksi Livingston yhtiön kehittämän RADIUS-palvelimen kanssa sekä myös Cistron RADIUS-palvelimen kanssa, josta FreeRADIUS haarautui ja sai alkunsa. Tosin verrattuna näihin mainittuihin palvelimiin FreeRADIUS tarjoaa huomattavasti laajemman määrän erilaisia mahdollisuuksia sekä ominaisuuksia. Lisäksi FreeRADIUS on erittäin helposti laajennettavissa sen avoimen rakenteen ja selkeän rajapinnan myötä. Lisäksi sen toiminta UNIX/Linux-ympäristössä mahdollistaa hyvin joustavan käytön. Käyttäjämäärältä FreeRADIUS voidaan skaalata toimimaan erittäin pienestä käyttäjämäärästä aina suurten käyttäjämäärien operaattoritason verkkoihin asti. [13. 77-78]

FreeRADIUS-projektin tuottaman järjestelmän käyttöönottoa helpottaa vilkas verkkoyhteisö sekä laaja käyttäjäkunta, joten moniin kysymyksiin sekä ongelmatilanteisiin saa helposti vastauksia. Toki koska kyseessä on avoimen lähdekoodin projekti, sen lähtökohtainen dokumentaatio ei välttämättä pysty

vastaamaan kaupallisten tuotteiden vastaaviin standardeihin. Onneksi tilannetta helpottaa se, että FreeRADIUS polveutuu hyvin selkeästi Cistron RADIUS projektista, joten sen dokumentaatio soveltuu osittain myös FreeRADIUS-palvelimen käyttöön. Tämä kuitenkin vain perustoiminnoissa, koska kyseinen projekti on kehittynyt huomattavasti siitä, kun se irtaantui Cistronin kehittämästä RADIUS-palvelimesta. Lisäksi laaja käyttäjäkunta pitää huolen siitä, että tarvittava tieto on helposti saatavilla verkkodokumenttien muodossa. [20.]

FreeRADIUS-palvelinta kehitetään GPL-lisenssin alla.

Poimintoja FreeRADIUS-palvelimen ominaisuuksista: [20.]

- monipuoliset toteutusmahdollisuudet AAA-prokollalle
- täysi tuki RFC 2865- sekä 2866-protokollille
- EAP, PEAP sekä Cisco LEAP -tuki
- tuki kaikille tunnetuille RADIUS-asiakastietokannoille
- joustava muokattavuus ja laajennettavuus
- tarvittaessa tuki erittäin suurelle käyttäjämäärälle

Tämän työn käytännön toteutukseen valittiin nimenomaan FreeRADIUS lähinnä sen takia, että se on kaikkein laajimmille levinnyt RADIUS-palvelimen toteutusratkaisu, ja siten se myös tarjoaa hyvän tukimahdollisuuden sekä dokumentaation. Lisäksi sen toiminta on täysin riittävä kyseiseen toteutustarpeeseen, koska se kattaa jopa operaattorin sisäisen verkon autentikointijärjestelmän, johon laajuuteen ei kuitenkaan tässä työssä mennä.

6.3.2 Open RADIUS

Toinen avoimeen lähdekoodiin perustuva suosittu RADIUS-palvelin on Open RADIUS. Kyseinen avoimen lähdekoodin palvelin kuuluu myös GPL-lisenssin alle, aivan kuten edellä esitelty FreeRADIUS.

Käytännössä eroavaisuudet edellä esiteltyyn FreeRADIUS-palvelimeen ovat rakenteellisesti melko pieniä, eli kyseinen projekti on myös hyvin yhteensopiva Livingstonin RADIUS-palvelimen kanssa, ja koska kyseessä on

UNIX/Linux ympäristössä käytettävä tuote, tukee se hyvin UNIX:in salasanatietokantoja.

Käytännössä siis ei ole suurta eroavaisuutta, valitaanko RADIUS-palvelimen toteutukseen FreeRADIUS vai OpenRADIUS, koska käytännössä molemmat sisältävät tarvittavat ominaisuudet sekä mahdollistavat melko vapaan ympäristön konfiguroida järjestelmä palvelemaan haluttua käyttötarkoitusta. [21.]

Poimintoja OpenRADIUS-palvelimen toiminnoista:

- tuki UNIX/Linux salasanatietokannoille
- vapaa muokattavuus käyttökohteen mukaan
- muokattavat autentikointijärjestelyt.

Kuten todettua OpenRADIUS on toiminnaltaan sekä ominaisuuksiltaan hyvin pitkälti vastaava FreeRADIUS-palvelimen kanssa, joten suuria eroja toimmoissa ei ole. [21.]

6.4 TACACS sekä TACACS+

Vaikka tässä työssä keskitytään nimenomaan RADIUS-palvelimeen ja toteuttamaan käyttäjän autentikointi RADIUS-palvelnta hyväksikäyttäen, on hyvä esitellä myös lyhyesti vaihtoehtoinen toteutusmalli käyttäjien autentikointiin.

TACACS on reitittimiä, kytkimiä sekä palvelimia valmistavan CISCO Systemsin kehittämä AAA-protokolla, josta on tällä hetkellä käytössä kolme eri versioita: TACACS, laajennettu TACACS sekä TACACS+. Näistä kaikkein kehittynein on TACACS+, joka on myös laajimmin käytetty versio.

Alkuperäinen TACACS-versio sisältää ainoastaan yksinkertaisen salasanan todennuksen sekä valtuutuksen. Tilastointi on hyvin suppea, eli se on rajoittunut ainoastaan valtuutuspyyntöjen kirjaamiseen. TACACS-järjestelmää kuitenkin laajennettiin, jonka jälkeen se korvasi alkuperäisen version. Nämä ensimmäiset versiot eivät kuitenkaan tukeneet AAA-protokollaa suoranaisesti, koska niiden tarjoama tilastointi oli niin heikkoa. TACACS+ on näistä versioista kaikkein pisimmälle jalostunut ja nykyisellään se tarjoaa jo yksityiskohtaisen tilastoinnin, joten se on tukee myös täysimittaisena AAA-protokollaa. [12. 119-122]

6.4.1 TACACS+ ja RADIUS

Molempien esiteltyihin protokollien (RADIUS ja TACACS+) toiminta kattaa samat AAA-protokollan sisältämät asiat, joten sinänsä ne tarjoavat yhdenmukaisen toimintamallin. Suurin ero niiden välillä on itse protokollissa, eli vaikka teknisesti ne tarjoavat lopputuloksena käytännössä samat palvelut, tulee palvelinten valinta miettiä käyttötarpeen mukaan. TACACS+ on keskitetty autentikointipalvelin, kun taas RADIUS perustuu asiakaspalvelinteknologiaan, ja on näin ollen soveltuva erilaisiin sekä erikokoisiin verkkoratkaisuihin pienyrityksistä aina operaattoritasolle asti.

Lisäksi eroa näiden palvelinten toiminnassa on yhteystekniikoissa, joissa TACACS+ käyttää TCP-protokollaa, kun taas RADIUS hyödyntää UDP-protokollaa. Näistä UDP-protokollaa pidetään suorituskykuisempänä siirtotienä kuin TCP:tä, mutta toisaalta TCP on luotettavampi.

TACACS+ suorittaa käyttäjän autentikoinnin sekä valtuutuksen erikseen, kun taas RADIUS yhdistää nämä kaksi vaihetta ja suorittaa ne samalla kertaa. Lisäksi eroa on käytettävässä salausmallissa, eli TACACS+ salaa koko viestin, kun taas RADIUS salaa ainoastaan annetun salasanan. [12. 119-122]

Oheiseen taulukkoon on kerätty vertailu kyseisten autentikointiprotokollien oleellisimmista eroavaisuuksista:

Taulukko 2. Autentikointiprotokollien eroavaisuudet

	RADIUS	**TACACS+**
Siirtotie	UDP (Suorituskykyinen)	TCP (Luotettava)
Salaus	Vain salasanan salaus	Koko viestin salaus
Todennus/Valtuutus	Salasanan ja tunnuksen todennus yhdistetty samaan palvelimeen	Mahdollisuus erottaa eri palvelimille
Käyttö	Kevyempi käyttää	Raskaampi, vaatii enemmän suorituskykyä laitteistolta

Muokattavuus	Avoin lähdekoodi, helppo muokata	Kaupallinen järjestelmä, jolloin rajoittuneempi muokattavuus

Käytännössä siis voidaan todeta, että RADIUS tarjoaa hieman yksinkertaisemman ja helpommin muokattavan autentikointiprotokollan, joka mahdollistaa joustavamman käytön verkkoympäristön mukaan. Lisäksi sen käyttämä siirtotie UDP on suorituskykyisempi kuin TACACS+:n käyttämä TCP. Tässä kuitenkin varjopuolena on UDP:n heikompi luotettavuustaso.

6.5 PAM

Jotta RADIUS-palvelimen yhteyteen kyetään liittämään mahdollisesti halutessa jotain autentikointia vahventavia lisälaitteita ja optimoimaan järjestelmän tietoturva, joudutaan ottamaan käyttöön PAM-moduulit, jotka ovat ulkopulisia järjestelmään liitettäviä osia jotka kontrolloivat yhteyksiä autentikointipalvelimien välillä.

PAM-moduulit mahdollistavat palvelimen autentikointiprosessiin liitettävän halutunlainen järjestelmän tietoturvaa lisäävä autentikointimoduuli, joka voi esimerkiksi olla jo aikaisemmissa kappaleissa esitelty muuttuvan kirjautumiskoodin tuottava esine tai biometriseen tunnistamiseen nojaava ratkaisu. [23.]

Tähän työhön valittu FreeRADIUS-palvelin on täysin PAM-yhteensopiva, eli sen asetustiedostot mahdollistavat autentikointiprosessiin liitettäväksi jonkin halutun ulkoisen autentikointiratkaisun.

PAM-moduulin toiminta perustuu siihen, että autentikointipalvelin kutsuu kyseisiä moduuleita, jotka on määritetty palvelimen autentikointiproesessin asetustiedostoihin. Tällöin kyseiset moduulit suoritetaan siinä järjestyksessä, jossa ne on määritelty suoritettavaksi, jonka jälkeen kyetään suorittamaan lopullinen käyttäjän tunnistus ja valtuuttaa käyttäjä oikein.

7 KÄYTÄNNÖN TOTEUTUS

Työn käytännön vaiheessa esitellään suunnitelma yrityksen sisäisen verkon toteutuksesta sekä siihen sisällytettävästä käyttäjien autentikointijärjestel-

mästä käyttäen AAA-protokollaa sekä sitä tukevaa RADIUS-palvelinta. Lisäksi käytännössä asennetaan RADIUS-palvelin ja testataan sen toiminta.

7.1 Suunniteltu järjestelmä

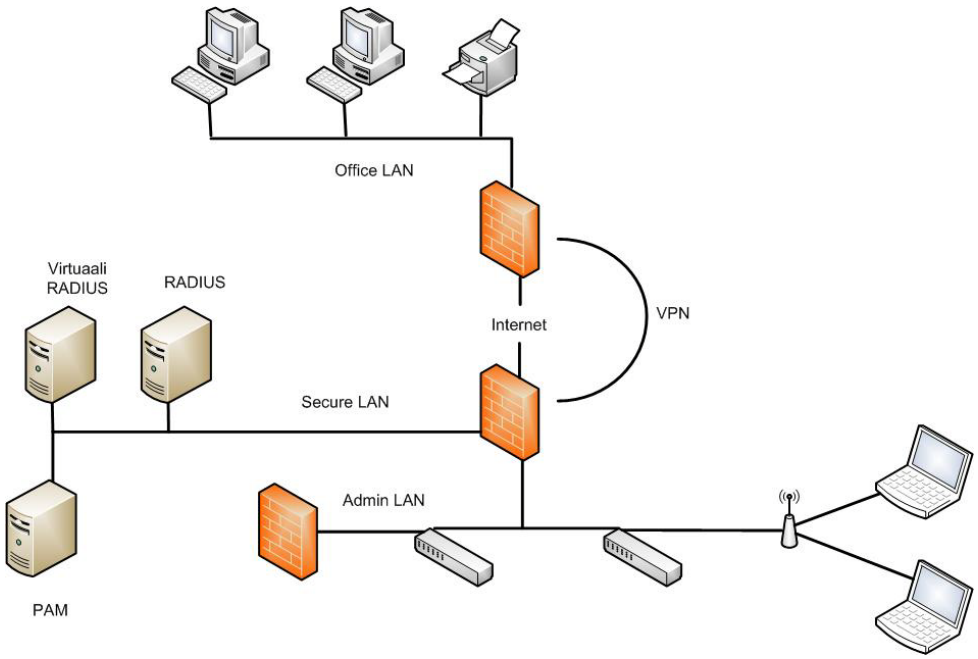
Kyseinen järjestelmä tullaan toteuttamaan tulevaisuudessa DataCenter Finland Oy:n toimesta käytännössä, mutta tässä kappaleessa esitellään suunnitelma tulevaisuudessa toteutettavasta verkkoratkaisusta sekä sen sisältämästä autentikointijärjestelmästä.

Kyseinen malli soveltuu noin 5-6 käyttäjän verkoksi, eli kyseessä on hyvin pieni yrityksen sisäinen verkko, johon toteutetaan käyttäjien autentikointijärjestelmä.

Kyseessä on toimiston sisäinen verkko, joka voidaan toteuttaa joko erillisenä verkkona tai virtuaalisena lähiverkkona jonkin toisen verkon sisälle. Autentikointi toteutetaan käyttämällä FreeRADIUS-autentikointipalvelinta. Verkkoon rakennetaan erikseen hallintaverkko, jolla pystytään seuraamaan verkon liikennettä sekä tekemään muutoksia verkon aktiivilaitteille. Tähän verkkoon annetaan pääsy ainoastaan verkon ylläpitäjälle. Eli peruskäyttäjälle ei ole pääsyä tekemään muutoksia verkon toimintaan. Tämän valvonta toteutetaan siis autentikointipalvelimella.

Autentikointipalvelin toteutetaan ns. ”kahdennettuna”, eli käytössä on kaksi identtistä palvelinta, joista toinen toteutuetaan virtuaalisesti. Tällöin kyetään säästämään kuluissa, mutta toiminnot pysyvät samanlaisina kuin varsinaisessa fyysisessä palvelimessa. Palvelimet on synkronoitu keskenään niin, että jokainen tapahtumat kirjautuvat molemmille autentikointipalvelimille, ja ongelmatilanteissa toisen palvelimen kaaduttua, toinen jatkaa toimintaansa normaalisti.

Suunniteltu verkko tulee sisältämään noin 20 erillistä laitetta (sisältäen käyttäjien omat tietokoneet), johon pääsy määritellään käyttäjän mukaan. Palvelinten ohjelmisto toteutetaan UNIX/Linux-pohjaisena, koska FreeRADIUS-palvelimen muokkaus ja käyttö on joustavampaa tässä ympäristössä.



Kuva 15. Suunnitelma järjestelmästä, johon RADIUS liitetään

7.1.1 Autentikointiprotokollan valinta

Kuten aikaisemmin on jo todettu, valitaan käytettäväksi autentikointiprotokollaksi RADIUS, ja sen avoimeen lähdekoodiin perustuva FreeRADIUS palvelin. Valintaan päädyttiin suunnitellun verkon käyttäjämäärän vuoksi, koska RADIUS tarjoaa noin 10 käyttäjän yritysverkkoon helposti toteutettavan autentikointiprotokollan, jonka muokattavuus, tietoturva sekä suorituskyky ovat riittävällä tasolla.

Vaikka RADIUS ei tarjoa salausta kuin salasanalla, voidaan sitä pitää tämän kokoisen verkon sisällä riittävänä, koska käyttäjämäärä ei nouse verkon sisällä kovin suureksi. Jos kyseessä olisi suurempi verkko sekä laajempi käyttäjämäärä, jouduttaisiin miettimään kokonaisen viestiliikenteen salaamista ja tällöin autentikointiprotokollaksi jouduttaisiin harkitsemaan TACACS+:aa. Tässä tilanteessa tulisi ottaa huomioon myös kasvavat kustannukset, koska TACACS+ on vahvasti sidoksissa CISCO Systemsin verkkolaitteisiin ja näin ollen mahdollisesti jouduttaisiin käyttämään ainoastaan yhden valmistajan laitteita.

7.1.2 Käyttäjä-autentikoinnin toteutus

Käyttäjän kirjautuminen verkkoon toteutetaan käyttämällä hallussa olevaa esinettä, joka generoi jokaisella kirjautumiskerralla uuden kirjautumisen mahdollistavan salasanan. Vaihtoehtona olisi myös biometrinen tunnistus,

joka toteutettaisiin kannettavan tietokoneen sormenjälkilukijalla, mutta koska kyseisen mallin valinta aiheuttaisi koko tietokonekannan uudistamisen, se tässä tapauksessa hylätään. Lisäksi kyseisen autentikointimallin yhdistäminen RADIUS-palvelimeen on vielä tässä vaiheessa turhan hankala toteuttaa, eikä sen aiheuttamat lisäkustannukset uusien laitehankintojen muodossa ei ole kyseisen verkon toteutuksen kannalta perusteltuja. Yksittäiselle työasemalle kirjautumiseen biometrinen sormenjälkitunniste toimii hyvin, mutta sen sovittaminen verkon tunniste-elementiksi ei ole tässä tapauksessa tarkoituksenmukaista.

Tämän myötä kustannustehokkain, tietoturvan kannalta sopiva sekä toteutukseltaan yksinkertaisin on hallussa olevaan esineeseen perustuva autentikointijärjestelmä. Tämän mallin toteuttamiselle on tarjolla esimerkiksi salasanan generoivia esineitä, kuten älykortteja tai avaimenperiä. Näissä ratkaisuissa kyseinen esine tulee olla aina käyttäjän mukana, jotta verkkoon kirjautuminen on mahdollista, mutta jos esine ei jostain syystä ole käyttäjän hallussa, myös verkkoon kirjautuminen on mahdotonta. Tämän takia nämä vaihtoehdot hylätään ja salasanan generointi suoritetaan matkapuhelimeen asennettavalla ohjelmistolla, jolloin käyttäjälle riittää että hänellä on mukanaan oma matkapuhelin. Kyseisessä mallissa rajoituksena on se, että puhelimen tulee tukea ulkopuolisia asennettavia ohjelmia.

Toisena vaihtoehtona salasanan hankintaan on tekstiviesti, eli käyttäjä lähettää tekstiviestillä pyynnön saada uuden OPM-salasanan. Tällöin käyttäjän tulee tietää myös järjestelmään oma pysyvä PIN-koodi, jolloin kirjautuminen perustuu kahteen eri tekijään:

- Johonkin, jonka käyttäjä tietää, eli ns. PIN-koodiin
- Johonkin, joka on käyttäjän hallussa, eli tässä tapauksessa matkapuhelimen kautta saatuun generoituun OPM-salasanaan.

Jotta tämä autentikointi saadaan järjestelmässä käyttöön, tulee RADIUS palvelimeen liittää ulkoinen PAM-moduuli, joka suorittaa käyttäjän autentikoinnin perustuen tähän generoituun salasanan sekä PIN-koodin yhdistelmään. Käytännössä ratkaisu toimii niin, että RADIUS kutsuu PAM-moduulia kun kirjautuminen suoritetaan, jolloin PAM-moduuli suorittaa käyttäjän syöttämän salasanan ja PIN-koodin tunnistuksen ja välittää tiedot RADIUS-palvelimelle, joka autentikoi käyttäjän.

Ohessa luettelo matkapuhelimeen perustuvan avainjärjestelmän tarjoajista jotka tukevat RADIUS-palvelinta:

- Aradiom
- AuthAnvil
- FireID
- FiveBarGate
- MobileOTP
- MobiSecure.

Avoimen arkkitehtuurin ratkaisun autentikointiin tarjoaa OATH-projekti, joka mahdollistaa hyvin joustavan autentikoinnin toteuttamisen erilaisissa ympäristöissä. OATH:hen pohjautuu esimerkiksi Visolve-projekti, joka tarjoaa avoimen ratkaisun muun muassa mobiililaitteisiin pohjautuvien salasanojen hallintaan ja tuottamiseen.

7.1.3 Verkon ja käyttäjien hallinta

Kuten yleisesittelyssä todetaan, verkko toteutetaan niin, että ylläpidolle annetaan oikeudet hallintaverkkoon, joka mahdollistaa pääsyn kaikkiin verkkolaitteisiin ja niiden asetuksiin. Lisäksi hallintaverkon kautta pystytään seuraamaan autentikointipalvelin toimintaa sekä tekemään siihen tarvittavia muutoksia. Muilla kuin hallintaverkkoon oikeutetuilla käyttäjillä ei ole pääsyä verkon aktiivilaitteisiin tai niiden asetuksiin. Näin ollen pystytään helposti rajaamaan käyttäjät sekä minimoimaan mahdolliset tietoturvariskit.

Vaikka RADIUS-palvelin asettetaan Linux-pohjaiseen järjestelmään, tullaan käyttäjätilastojen kerääminen toteuttamaan Windows Server -järjestelmän Active Directory -käyttäjätietokannalla, koska verkkoa käytetään ja ylläpidetään Windows-ympäristössä. Jotta autentikointipalvelimen toiminta saadaan mahdollisimman aukottomaksi, järjestelmä toteutetaan niin kutsutusti kahdennettuna, jolloin jokainen tehty muutos näkyy välittömästi molemmissa järjestelmissä. Palvelimet ovat toiminnoiltaan identtiset. Ainoastaan toteutus eroaa siinä, että toinen on fyysinen palvelin ja toinen virtuaalisesti toteutettu. Näin ollen saadaan sama tulos, mutta lisätään kustannustehokkuutta.

7.2 RADIUS-palvelimen asennus

Palvelimen testausympäristönä toimii VMWare Worstation 7.0 -ohjelmistolla virtualisoitu Linux-palvelin, johon on asennettuna Ubuntu Linux 9.10. Ubuntu valittiin testiympäristöksi sen helpon käyttöönoton takia. Todellisuudessa palvelimesssa tullaan todennäköisesti käyttämään jotain muuta Linux-jakelua, mutta koska Ubuntu on Debian-pohjainen jakelu, ja sillä on hyvä tuki RADIUS-palvelimelle, voidaan todeta, että testiympäristössä suoritettava asennus ja testaus vastaa täysin ympäristöä, jossa käytössä on joku toinen paremmin palvelinympäristöön sopiva Linux-jakelu.

Kuten edeltävässä kappaleessa todettiin, valittiin asennettavaksi RADIUS-palvelimeksi vapaaseen lähdekoodiin perustuva FreeRADIUS. Palvelin on saatavissa Ubuntun Synpatic Package Manager paketinhallinta-ohjelmiston kautta. Ohjelman haku ja asennus tapahtuu konsolissa seuraavalla:

Jotta järjestelmä antaa käyttäjälle ns. root-oikeudet, tulee käskyjen edessä käyttää komentoa ”sudo”.

Aluksi haettiin viimeisimmät käyttöjärjestelmän päivitykset komennolla

sudo apt-get update

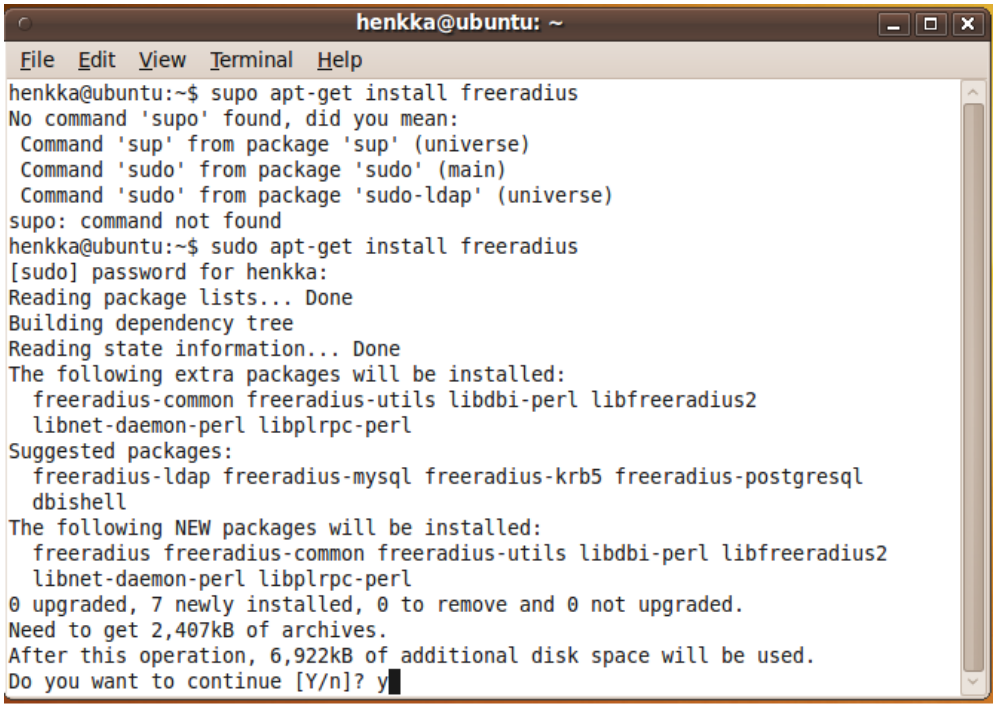
Tämän jälkeen, kun järjestelmä on päivittänyt itsensä, etsittiin pakettienhallinnasta tarjolla olevat RADIUS-palvelimet komennolla

sudo apt-cache search radius

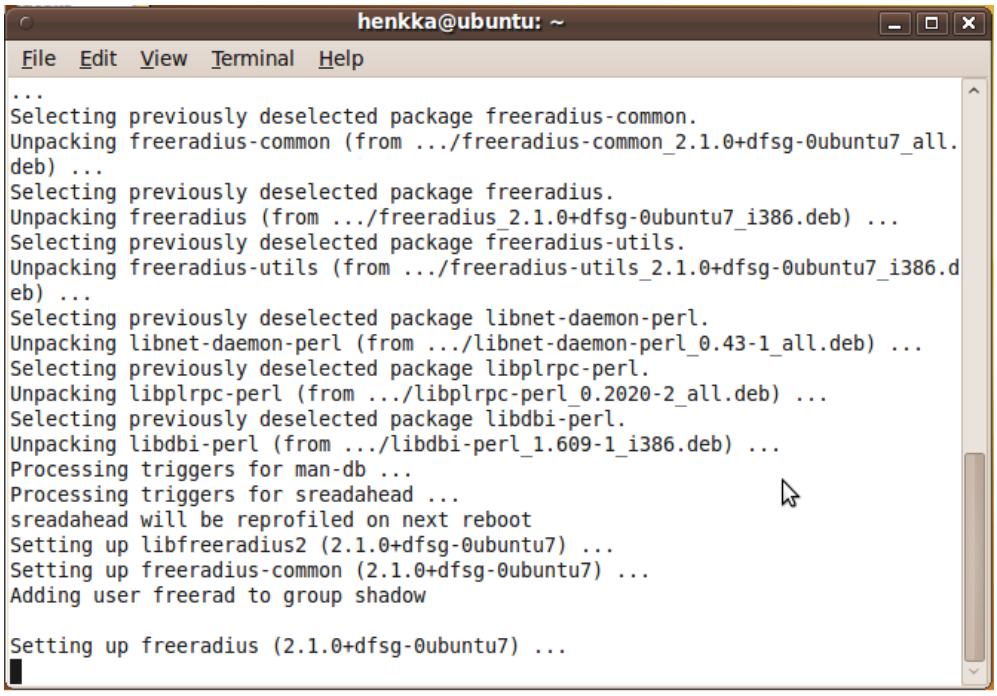
Tämän jälkeen suoritettiin FreeRADIUS-ohjelmiston asennus komennolla

sudo apt-get install freeradius

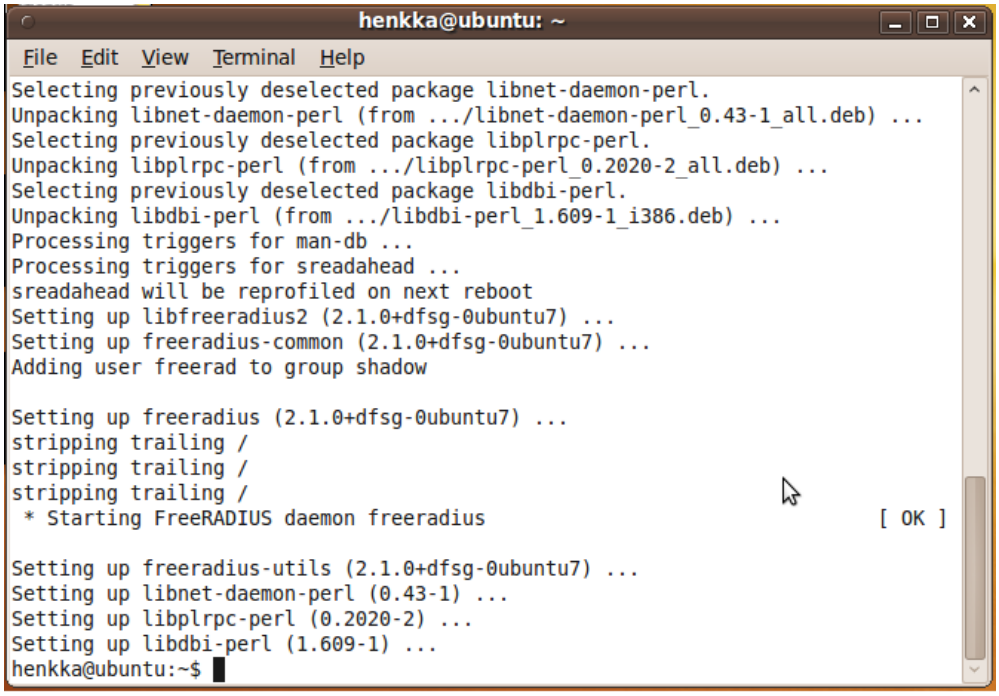
Kuvissa 15-17 on esiteltynä FreeRADIUS-palvelimen asennusprosessi.



Kuva 15. FreeRADIUS-palvelimen asennus 1



Kuva 16. FreeRADIUS-palvelimen asennus 2



Kuva 17. FreeRADIUS-palvelimen asennus 3

Kyseisen komennon jälkeen FreeRADIUS asentui virtuaalikoneelle ja tämän jälkeen käynnistyi automaattisesti ilman erillistä käynnistyskomentoa. Tämän myötä kyseisessä koneessa oli käynnistyneenä RADIUS-palvelin, jonka asetuksia päästään muokkaamaan. Ilman asetusten muokkaamista kyseinen palvelin ei kykene vielä suorittamaan minkäänlaista käyttäjän tunnistusta tai valtuutusta, koska mitään parametrejä tai käyttäjien tietoja ei ole annettu järjestelmään.

7.3 Asetusten muokkaus

Tässä kappaleessa esitellään FreeRADIUS-palvelimen toimintakuntoon saattamisessa tärkeimmät asetustiedostot, niiden toiminta ja tarkoitus sekä niihin testivaiheessa tehtävät muutokset ja lisäykset.

7.3.1 radiusd.conf

Radiusd.conf-tiedosto on koko palvelimen asetusten kannalta tärkein tiedosto, koska se määrittelee asennetun RADIUS-palvelimen kaikki yleiset asetukset. Kyseinen tiedosto sekä muut palvelimen toiminnan kannalta olennaiset sekä muokattavat tiedostot sijaitsevat yleisesti kansiossa */etc/freeradius.*

RADIUS-palvelimen ensikäynnistyksen kannalta tärkeimmät asetukset ovat eri tietojen sijainnit, joista palvelin osaa ne etsiä. Ilman näiden tietojen oikeellisuutta palvelinta ei saada käynnistettyä.

Kyseiset tiedot, jotka tulee tarkistaa ovat *passwd, shadow* sekä *group*. Nämä löytyvät radiusd.conf-tiedoston ”Unix” -osioista, josta ne asennuksen jälkeen tarkistettiin ja todettiin niiden olevan merkittynä kommenteiksi. Kun ne poistettiin, saatiin määriteltyä niiden sijainnit oikein. Näin palvelimen käynnistyminen on mahdollista.

Ohessa listaus asetettavista arvoista:

passwd = /etc/passwd

shadow = /etc/shadow

group = /etc/group

7.3.2 clients.conf

Kyseinen *clients.conf*-tiedosta sisältää palvelimen tarvitsemat tiedot kaikista siihen yhteyttä ottavista käyttäjistä. Nämä tiedot ovat esimerkiksi salasanatietoja sekä jaettuja salaisuuksia, joilla yhteys palvelimeen otetaan.

Tiedostossa on jo valmiiksi tietoja esimerkkiasiakkaista, joten asetusten määrittäminen on sen myötä melko helppoa. Tärkein huomioitava asia on, että jaetun salaisuuden tiedot ovat keskenään samat asiakkaiden tietojen kanssa, koska muuten yhteyden ottaminen ei onnistu.

Testissä käytetty esimerkki asiakkaan tiedoista:

Client 192.168.1.0/16

secret = hftestiverkko

shortname = hftv

Kyseisissä tiedoissa, jaettu salaisuus on ”hftestiverkko” ja asiakkaan nimi ”hftv”. Testiyhteyttä otettaessa pitää siis tietää tuo määritelty jaettu salaisuus.

7.3.3 users

Edellisessä kappaleessa esitelty *clients.conf*-tiedosto sisälsi asiakaskoneiden tietoja, mutta nyt esiteltävä *users*- tiedosto pitää sisällään käyttäjien tunnistetietoja, joilla käyttäjän autentikointi on mahdollista. Jos kyseiseen tiedostoon ei tehdä muutoksia, käyttää RADIUS-palvelin lähtökohtaisesti ainoastaan Uinx/Linux-salasanojen tietokantaa, jolloin tietoturva ei tietenkään ole kovin hyvällä tasolla. Tällöin myöskään yhdellä käyttäjälle ei käytössä ole kuin yksi samanaikainen kirjautuminen palvelimelle.

Tämä kuitenkin toimii testiympäristössä, mutta yrityskäyttöön toteutettavassa järjestelmässä vaaditaan tarkemmat tunnistetiedot, jolloin ne sijoitetaan tähän kyseiseen *users*-tiedostoon.

7.3.4 Muut asetustiedostot

Edellisten esiteltyjen asetustiedostojen lisäksi, RADIUS-palvelimen toimintaan vaikuttavia tärkeitä tiedostoja ovat *naslist-, hints*- sekä *huntgroups-tiedostot.*

Naslist-tiedosto voidaan määritellä kaikki NAS-liityntäpisteiden tiedot, jotka ottavat yhteyden autentikointipalvelimeen. Näitä tietoja ovat esimerkiksi laitteen nimi sekä tyyppi.

Hints-tiedosto pitää sisällään sisältää tiedot, kuinka palvelin käsittelee asiakkaiden käyttäjänimiä, sekä sisältää ns. ”vihjeitä”, kuinka palvelin jakaa oikeuksia käyttäjänimien perusteella. Tämä on hyvin tärkeä vaihe eritoten jos oikeuksia jaetaan verkon sisällä eri käyttäjille, jotta pystytään määrittämään mihin laitteisiin ja verkon osiin käyttäjällä on oikeus päästä.

Huntgroups-tiedosto sisältää tiedot järjestelmässä käytettävistä porteista joiden kautta kommunikointi asiakkeiden ja autentiointipalvelimen välillä tapahtuu. Kyseisessä tiedostossa voidaan määritellä esimerkiksi porttiperusteisesti määrittelemään yhteydenottajat ja mihin verkon osiin käyttäjä pääsee kirjautumaan.

Nämä kaikki esitellyt tiedostot sijaitsevat */etc/freeradius*-kansiossa.

7.4 Testaus

Ensin testattiin palvelimen perusasetusten virheettömyys ajamalla *radiusd daemon*-testausohjelma, jolla *radiusd.conf* -tiedoston asetukset voidaan

varmistaa, että annetut parametrit tiedostossa on oikein. Kyseinen toiminto suoritettiin testissä seuraavasti:

radius:/etc/freeradius # radiusd

radiusd: Starting – reading configuration files …

radius: etc/freeradius #

Koska järjestelmä ei antanut mitään varoituksia, voidaan todeta että RADIUS-palvelin on toiminnassa.

Asiakastietojen lisäys toteutettiin clients.conf tiedostoon niin, että yhden esimerkkiasiakkaan tiedoista poistettiin kommenttimerkit, jonka jälkeen sen tiedot vaihdettiin vastaamaan kyseistä testitilannetta:

client 192.168.1.0/8

secret = hftestiverkko

shortname = hftv

Kun testiasiakkaan tiedot on määritelty järjestelmään, tulee määritellä portti, jotan autentikointipalvelin kuuntelee yhteyttä otettaessa. RFC 2138-standardi määrittää RADIUS-palvelimen standardiksi portin 1812, joten testissä käytettiin tätä porttia. Jotta pelvelin saadaan kuuntelemaan ko. haluttua porttia, tulee se käynnistää uudestaan *radiusd*-komennolla seuraavasti:

radius:/etc/freeradius # radiusd –p 1812

radiusd: Starting – reading configuration files …

radius: etc/freeradius #

Kyseinen portti on määritelty palvelimen perusasetuksissa kuunneltavaksi portiksi, mutta näin ollen asia pystyttiin vielä varmistamaan.

Itse käyttäjän kirjautuminen testataan *radtest*-ohjelmalla, joka asentuu yhdessä palvelimen kanssa.

Testaus toteutetaan seuraavasti:

radtest henkka hftestiverkko testi 1812 testiverkko

jossa:

henkka = käyttäjätunnus

hftestiverkko = salasana (jaettu salaisuus)

testi = asiakas

hftestiverkko = salasana

Tämän jälkeen palvelin antoi Access-Accept vastauksen, jolloin voitiin todeta että kirjautuminen kyseisillä arvoilla onnistui palvelimelle. Väärillä tunnuksilla palvelin vastasi Access-Reject vastauksella, jolloin kirjautuminen ei tietenkään onnistunut.

8 YHTEENVETO

Tässä insinöörityössä perehdyttiin AAA-protokollaan sekä sen toteuttamiseen käyttämällä RADIUS-autentikointipalvelinta. Alussa käytiin läpi perustiedot eri verkkoteknologioista sekä yleensä yrityksen verkkoratkaisuissa käytettävästä virtuaalisesta lähiverkosta. Lisäksi esiteltiin eri autentikointiprotokollat, joihin käyttäjien tunnistus, valtuutus sekä käyttäjätietojen tilastointi perustuu sekä erilaiset tunnistamiseen käytettävät toteutusvaihtoehdot. Käyttäjän tunnistamisen toteutusvaihtoehdoista esiteltiin salasanaan, käyttäjän hallussa olevaan esineeseen sekä biometriseen tunnistamiseen perustuvat ratkaisut.

Työssä keskityttiin nimenomaan tutkimaan verkkoratkaisuita niin, että niihin kyetään integroimaan autentikoinnin suorittava palvelinratkaisu, joka tässä työssä valittiin toteutettavaksi vapaan lähdekoodin FreeRADIUS-palvelimella.

Teorian lisäksi työssä asennettiin virtuaaliseen verkkoympäristöön FreeRADIUS-palvelin ja testattiin sen asetusten määrittäminen ja näiden toimenpiteiden jälkeinen toiminta.

Työn perusteella voidaan todeta että RADIUS-palvelin mahdollistaa erittäin joustavan käyttäjä-autentikoinnin toteuttamisen esimerkiksi pienen toimiston sisällä, jossa halutaan määritellä käyttäjille verkon sisällä erilaisia valtuuksia tehdä toimenpiteitä tai jakaa tiedostoja käyttäjien kesken hallitusti. Lisäksi

siihen liitettävän matkapuhelimella generoitavan salasanaan perustuvan autentikointiratkaisun myötä voidaan taata verkolle tarpeeksi hyvä tietoturva.

VIITELUETTELO

[1] Hämeen-Anttila, Tietoliikenteen perusteet, Docondo Finland, Jyväskylä, 2003.

[2] Jaakkohuhta, Lähiverkot – Ethernet, Edita, Helsinki, 2000.

[3] Hakala, Vainio, Tietoverkon rakentaminen, Docondo Finland, Jyväskylä, 2005.

[4] IEEE, 802.1q Standard [Verkkodokumentti]. IEEE Standard kotisivu. [Viitattu 15.11.2009] Luettavissa: http://standards.ieee.org/reading/ieee/std_public/description/lanman/802.1q-2003_desc.html.

[5] Seppänen, Ongelmallinen Ethernet [Verkkodokumentti]. VTT kotisivu. [Viitattu 20.10.2009] Luettavissa: http://iplu.vtt.fi/lopsem07/paatosseminaari-ethernet.pdf.

[6] Mayers, VERKOT Sertifikaatti s. 503-505. EDITA, Helsinki, 2003.

[7] Simpson, The Point-to-Point-Protocol [Verkkodokumentti]. IETF kotisivu. [Viitattu 20.10.2009] Luettavissa: http://www.ietf.org/rfc/rfc1661.txt.

[8] Simpson, PPP LCP Extensions [Verkkodokumentti]. IETF kotisivu. [Viitattu 20.10.2009] Luettavissa: http://tools.ietf.org/html/rfc1570.html.

[9] Lloyd, Simpson, PPP Authentication Protocol [Verkkodokumentti]. RFC Tietokanta. [Viitattu 20.10.2009] Luettavissa: http://www.faqs.org/rfcs/rfc1334.html .

[10] Simpson, CHAP Authentication Protocol [Verkkodokumentti]. RFC Tietokanta. [Viitattu 20.10.2009] Luettavissa: http://www.faqs.org/rfcs/rfc1994.html.

[11] Puska, Langattomat Lähiverkot s.75-77. Gummerus, Jyväskylä, 2005.

[12] Thomas, Verkkojen tietoturva, Edita, Helsinki, 2005.

[13] Hassell, RADIUS, O´Reilly Media, 2003.

[14] Brownlee, Blount, Accounting Attributes and Record Formats [Verkkodokumentti]. RFC Tietokanta. [Viitattu 22.10.2009] Luettavissa: http://www.faqs.org/rfcs/rfc2924.html.

[15] Ojala, Tietoturva [Power Point-esitys]. Turun AMK kotisivu. [Viitattu 2.11.2009] Luettavissa: http://www.dc.turkuamk.fi/users/mmakela/Narikka/Internet-tekniikan%20perusteet/tietoturva.ppt.

[16] Koskinen, Tietoturvaprotokollia [Verkkodokumentti]. Turun TKK:n kotisivu. [Viitattu 2.11.2009] Luettavissa: http://www.cs.tut.fi/kurssit/8306000/pr.html.

[17] Biometriikka. [web-sivu]. Turun TKK:n kotisivu. [Viitattu 2.11.2009] Luettavissa: http://sec.cs.tut.fi/maso//teksti.php?id=201.

[18] Ylä-Jääski, Internet lähiverkoksi [verkkolehti]. MicroPC 14/2001. [Viitattu 5.11.2009] Luettavissa: http://mikropc.net/nettilehti/pdf/pc2009200140.pdf.

[19] Rigney, Simpson, RADIUS [Verkkodokumentti]. IETF kotisivu. [Viitattu 5.11.2009] Luettavissa: http://www.ietf.org/rfc/rfc2865.txt.

[20] FreeRADIUS, FreeRADIUS Wiki [web-sivu]. FreeRADIUS kotisivu. [Viitattu 15.11.2009] Luettavissa: http://wiki.freeradius.org/Main_Page#Overview.

[21] OpenRADIUS, OpenRADIUS introduction [web-sivu]. OpenRADIUS kotisivu. [Viitattu 17.11.2009] Luettavissa: http://www.xs4all.nl/~evbergen/openradius-index.html/.

[22] MySQL, Why MySQL [web-sivu]. MySQL kotisivu. [Viitattu 19.11.2009] Luettavissa: http://www.mysql.com/why-mysql/.

[23] Linux Kernel, PAM FAQ [verkkodokumentti]. kernel.org kotisivu. [Viitattu 24.11.2009] Luettavissa: http://www.kernel.org/pub/linux/libs/pam/FAQ.